ABLELink®

EH6508G Industrial Managed Switch Series

User Manual

Version 1.1

March, 2008

atop Technologies

TEL: +886-3-5508137

FAX: +886-3-5508131

http://www.atop.com.tw

Important Announcement

The information contained in this document is the property of Atop Technologies, Inc. and is supplied for the sole purpose of operation and maintenance of products of Atop Technologies, Inc. No part of this publication is to be used for any other purposes, and it is not to be reproduced, copied, disclosed, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form, by any means, in whole or in part, without the prior explicit written consent of Atop Technologies, Inc.

Published by

Atop Technologies, Inc.

2F, No. 146, Sec. 1, Tung-Hsing Rd.
Jubei, Hsinchu 30261
Taiwan, R.O.C.
Tel: 886-3-5508137
Fax: 886-3-5508131
www.atop.com.tw

Copyright © 2007 Atop Technologies, Inc. All rights reserved.
All other product names referenced herein are registered trademarks of their respective companies.

Table of Contents

ABLELink® i
EH6508G Industrial Managed Switch Series i
User Manual i
About this Manual 1
Packing List 1
Part 1 Know Your Atop's ABLELink® EH6508G Switch 2
1.1 What is a Managed Industrial Switch 2
1.2 Software Features 2
1.3 Hardware Features 3
1.4 Hardware Installation 4
1.5 Hardware Overview 6
Part 2 Configuring with a Web Browser 12
2.1 Web-based Management Basics 12
2.2 Defauts 12
2.3 Login and Main Window Interfaces 12
2.4 Basic Settings 13
2.5 Port Configuration 23
2.6 Redundancy 26
2.7 VLAN 30
2.8 Traffic Prioritization 34
2.9 IGMP Snooping 36
2.10 SNMP Configuration 37
2.11 Security 39
2.12 Warning (Fault Alarm Messages) 44
2.13 Monitor(ing) and Diag(nosis of Individual Port) 49
2.14 Front Panel 52
2.15 Save Configuration 52
Part 3 Configuration via Command Line Interface (CLI) 53
The EH Series supports Configuration by the Command Line Interface or CLI. The user may manage the switch via its console port or via Telnet. 53
3.1 CLI Management via a PC's Serial-console Port 53
3.2 CLI Management via Telnet 56
3.3 CLI List of Commands 57
Appendix: Configuring with Atop's Utility Software: EtherManager 70
A.1 EtherManager Basics 70

A.2 Tasks and Functions.....74
A.3 All-Functions Interfaces.....84
EH6508G Technical Specifications.....86

About this Manual

This manual is divided into three parts. **Part 1** covers the hardware descriptions of the EH6508G Series. **Part 2** gives a function-by-function description of the **Web-based** management approach, while **Part 3** describes the steps for configuring via a PC's serial port of via **Telnet** (Command Line Interface or **CLI**).

A utility program **EtherManager** and its settings are included in the **Appendix.**

At the end of this manual is the EH series **Product Specifications**.

Packing List

Inside the Package please find:

- Atop EH6508G Industrial Managed Switch x1
- 7-pin Terminal Block for two external powers & relay connections x1
- Port Plugs (8 RG-45 plugs for EH6508G, and 6 RG-45 covers and 2 SC fiber port covers for EH 6508G-Fm or EH6508G-Fs)
- Wall mount kit x1
- Atop Industrial Managed Switch quick start guide x1
- Product CD with configuration utility EtherManager x1
- Product Warranty x1

Part 1 Know Your Atop's ABLELink® EH6508G Switch

1.1 What is a Managed Industrial Switch

Atop's ABLELink® EH (**E**thernet Switching **H**ub) 6508G series consists of powerful managed industrial switches. A switch is referred to as an OSI Layer 2 bridging device. Unlike an "**unmanaged**" switch which is normally found in homes or in small SOHO environments and runs in "auto-negotiation" mode, each port on a "**managed switch**" can be configured in its link bandwidth, priority, security, and duplex setting. The managed switches can be configured and managed remotely via **the Web**, **TELNET** or via a serial port of a computer. The series also comes with an ATOP proprietary utility software **EtherManager** that allows the user to configure multiple switches at the same time. While used in a complex ring configuration, the EH series offers an "**iA-Ring"** topology which boasts a fast recovery time of less than 10 ms.

The EH series is also an industrial switch (as opposed to a commercial switch) in its ruggedized packaging to operate in a harsh industrial environment: extreme temperature, high humidity, dusty air, potential high impact and the presence of potentially high static charges.

The series is furnished with two Gigabit ports (copper) for high-speed transmission needs or two fiber ports for high-speed-and-long-distance transmission needs.

The EH series belongs to the category of Managed Industrial switches, and is designed to be physically and electrically robust, and yet user-friendly.

1.2 Software Features

- Atop's **iA Ring** topology offering Network redundancy and fast recovery (<10ms)
- **"iA Ring**" supporting Ring Coupling and Dual Homing
- Compliant with **SNMP**v1/v2/v3 & RMON & Port base/802.1Q VLAN Network Management
- Event notification by Email, **SNMP** trap and Relay closing
- Three approaches: **Web-based** ,**CLI** (Serial-console port and Telnet), and EtherManager
- Redundant (total three) DC power inputs: 2 inputs at the terminal block & 1 at the separate power jack
- **MAC-based** port security
- **Port-based** network access control :802.1x
- **VLAN** (802.1Q) for traffic segregation and network security
- **802.1x-Radius** centralized password management
- **SNMP**v3 encrypted authentication and access security

- **RSTP** (802.1w) supported
- **QoS** (802.1p) real-time traffic regulation
- **VLAN** (802.1Q) with double tagging and GVRP support
- **IGMP Snooping** for multicast filtering
- Individual port configuration: status, statistics, mirroring, security
- Remote Monitoring (**RMON**)

1.3 Hardware Features

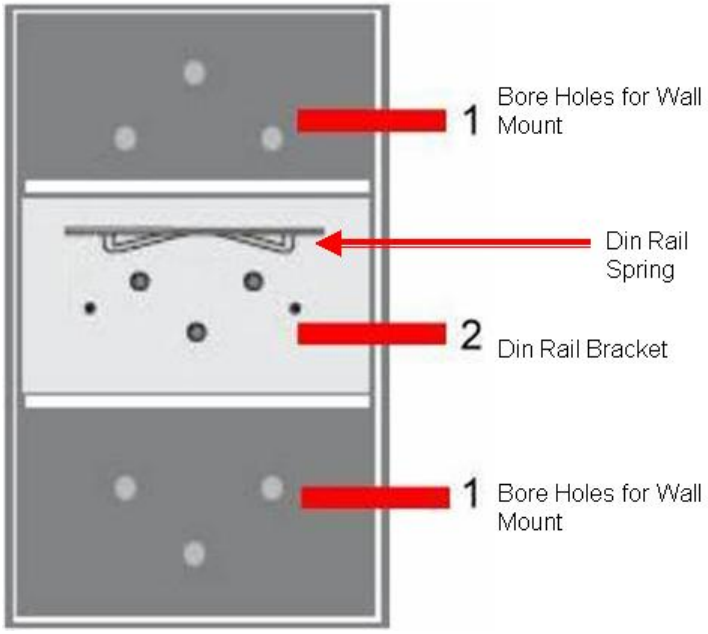
- Dual DC inputs (12 to 48VDC)
- Redundant third DC power jack
- Operating Temperature: -10 to60 ℃
- Storage Temperature: -40℃ to 85℃
- Operating Humidity: 5% to 95%-Non-condensing
- IP-30 casing
- 2x Gigabit Ethernet ports or 2x Fiber ports
- 6 x 10/100M Ethernet ports
- Serial-Console Port in **CLI** Configuration
- Dimensions: 52 mm (W) x 106 mm (D)x 144 mm (H)

1.4 Hardware Installation

1.4.1 INSTALLATION ON "DIN RAIL"

All EH Switches are equipped with a din-rail bracket attached onto the rear panel. Follow the steps below to fasten the switch to the din rail.

Step 1: Tip the switch forward and press it against the din rail after align the bracket springs to the din rail

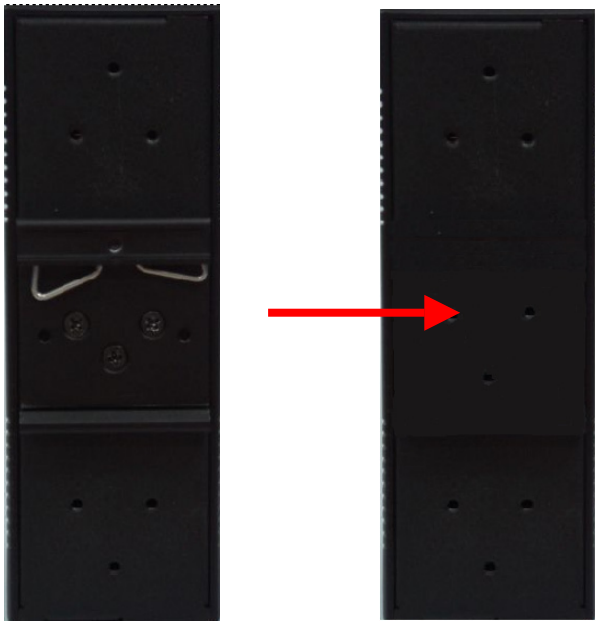


Step 2: Press the bracket against the upper ledge of the din rail until it clicks

1.4.2 INSTALLATION WITH WALL-MOUNT PLATE

A wall-mount plate furnished in the package is for fastening the switch onto a wall.

Step 1: Remove the din rail bracket from the back panel of the switch



Step 2: Use the 6 machine screws to attach the wall-mount plate to the back of the switch

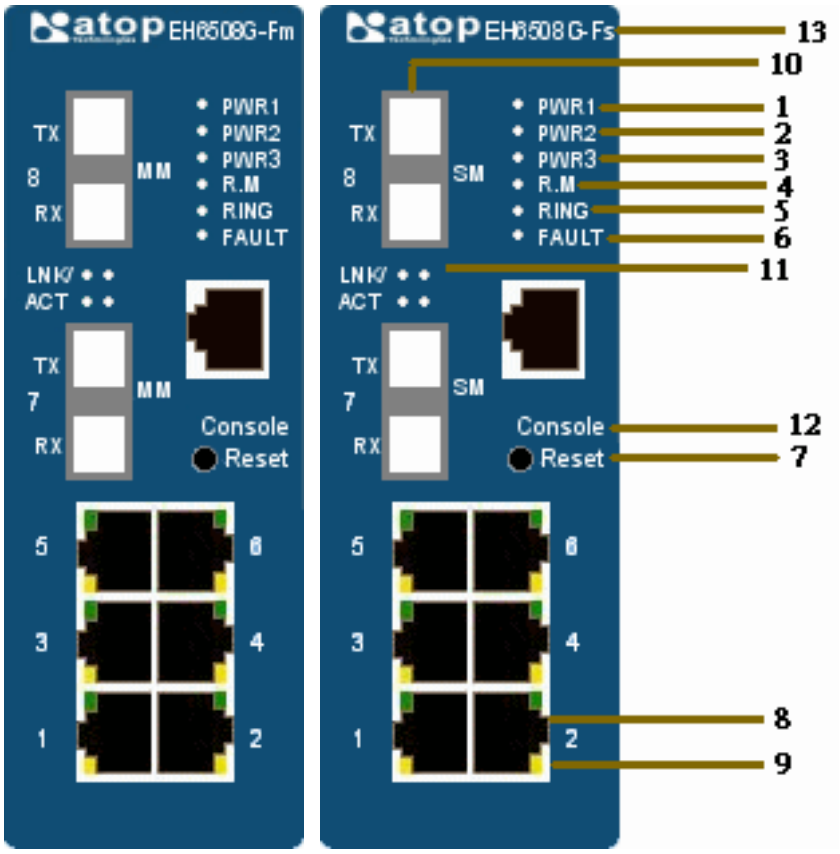
Step 3: Mount the combined assembly onto the wall

1.5 Hardware Overview

1.5.1 FRONT PANEL

a. EH6508G-Fm or EH6508G-Fs Models

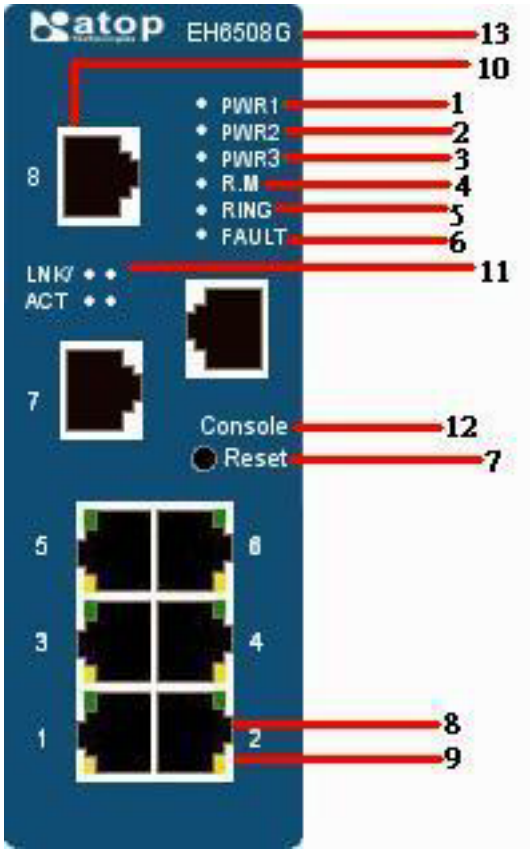
EH6508G-Fm/Fs



1. When **PWR1** is in, the green LED lights up
2. When **PWR2** is in, the green LED lights up
3. When the **PWR3** is in, the green LED lights up
4. The green **R.M**. LED light comes on when the switch is the Ring Master of an iA-Ring
5. The RING LED comes on when the iA-Ring is active
6. The amber FAULT LED comes on when a fault is detected (see 2.12.1 for fault definition)
7. Press the Reset bottom for 5 seconds to set the switch to the factory defaults
8. 10/100Base-T Ethernet ports (1-6)
9. LEDs for Ethernet ports status (1-6): LNK (steady amber) and ACT (blinking green)
10. 1000Base-SX (multi-mode) or 1000 Base-LX (single-mode) fiber ports
11. Fiber Port Status Indicators; 2 sets, with the upper set for port 8: on the left being the LNK indicator (amber) and on the right, ACT indicator (blinking green)
12. Console port (for serial port connection) for CLI Management
13. Model name

b. EH6508G Model

EH6508G



1. When PWR1 is in, the green LED lights up
2. When PWR2 is in, the green LED lights up
3. When the PWR3 is in, the green LED lights up
4. The green R.M. LED light is on when the switch is the Ring Master of an iA-Ring (Normally off until the Ring Master function is defined)
5. The RING is on when the iA-Ring is active (Normally off until an iA Ring is defined)
6. The amber FAULT is on when a fault has been detected (see 2.12.1 for fault definition)
7. Pressing the indented Reset bottom with the tip of a paper clip for 5 seconds to set the switch to the factory defaults
8. 10/100Base-T Ethernet ports (1-6)
9. LED for Ethernet ports status (1-6)
10. 10/100/1000BaseTX Giga ports (7 and 8)
11. Status LEDs for the Gigabits ports; 2 sets, with the upper set for port 8: on the left being the LNK indicator (amber) and on the right, ACT indicator (blinking green)
12. Serial-Console port (RJ-45)
13. Model name

Port	Description
10/100 RJ-45 Fast Ethernet ports (6)	6 10/100Mbps RJ-45 fast Ethernet ports supporting auto-negotiation **Default Setting:** Speed: auto Duplex: auto Flow control : disable
Gigabit port (2) or Fiber port (2)	2x1000 Base-T Giga ports, copper wires (EH 6508**G**) Or 1000Base-SX for EH 6508G-Fm (m for multi-mode at 850 m 1000Base-LX for EH 6508G-Fs (s for single mode at 1310 m)
Console port (1)	For configuring switch using PC's serial port. The console port itself is a RJ-45 connecter. Note: The serial-to-RJ-45 conversion cable-connector can be order through Atop.
Reset button (1)	Push 5 seconds to reset switch to **Factory Defaults**

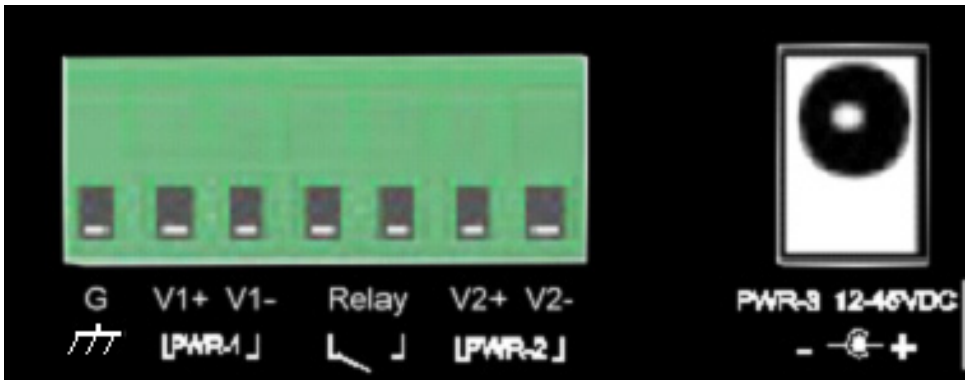
1.5.2 LED INDICATORS

LED	Color	Status	Description
PW1	Green	On	DC power module 1 in place
PW2	Green	On	DC power module 2 in place
PW3	Green	On	Third power Input (from power jack) in place
R.M.	Green	On	IA-Ring Master designated
RING	Green	On	IA-Ring enabled
		Slow blinking (~1Hz)	IA-Ring with only one link (lacking the third link to form a ring.)
		Fast blinking (~3 Hz)	IA-Ring functioning normally.
FAULT	Amber	On: Fault event(s) detected Off: Operation normal	(see 2.12.1 for Fault Alarm settings)
10/100 Fast Ethernet ports			
ACT	Green	Blinking	Transmission normal
LNK	Amber	On	Port link normal
Gigabit Ethernet ports (7 and 8)			
ACT	Green	Blinking	Transmission normal
LNK	Amber	On	Port link normal
Fiber ports (7 and 8)			
ACT	Green	Blinking	Transmission normal
LNK	Amber	On	Port link normal

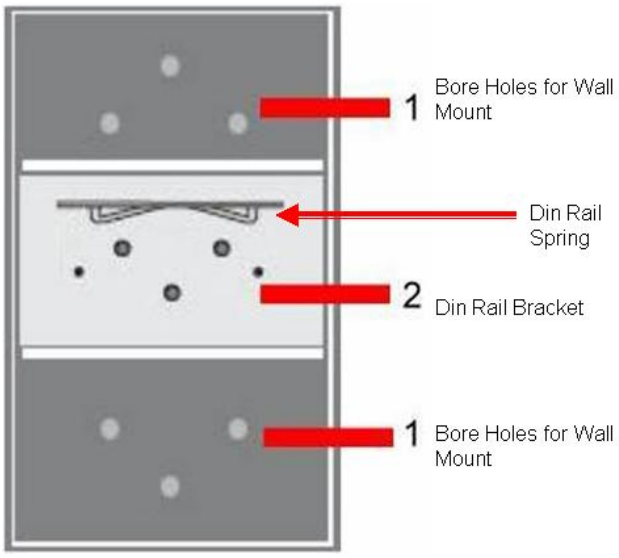
1.5.3 BOTTOM PANEL AND TERMINAL BLOCK

The bottom panel consists of a terminal block for dual power inputs and a separate power jack for further redundancy.

1. Terminal block that includes: PWR1, PWR2 (12-48V DC) inputs and a Fault Relay (normally open, supporting 1A @ 120 VAC or 2A @ 24 VDC) which is forced to close in case of a fault event



1.5.4 Rear Panel and Wall-Mount Bracket



1.5.5 Serial-Console Port Pin Assignments

The EH series can be managed via the **console port** (note: it is an RJ-45 connector) from a PC's serial port and is also referred to as the **serial-console port**. The serial to RJ-45 connector pin assignment are shown as below. The serial-to-RJ45 cable connector can be ordered through Atop if needed.

Serial-Signal	RJ 45
TxD	Pin #2
RxD	Pin #3
GND	Pin #5

1.5.6 Ethernet Port Cables, Transmission Distances and Connector Types

The EH switches are equipped with 6 standard Ethernet RJ-45 ports. Either CAT 3, 4, 5 or 5e UTP cables can be used to connect other network devices: PCs, servers, switches, routers, or hubs. The following table stipulates their typical transmission distances.

■ Cable Types and Maximum Transmission Distance

Cable	Type	Max. Transmission Length	Connector Types
10BASE-T	Cat. 3, 4, 5 UTP	100 m	RJ-45
100BASE-TX	Cat. 5 UTP	100 m	RJ-45
1000BASE-TX	Cat. 5/Cat. 5e UTP	100 m	RJ-45

Cable specification table

1.5.7 RJ-45 Pin Assignments

On the RJ-45 connector, pins 1 and 2 are for transmitting data, and pins 3 and 6 for receiving data.

■ RJ-45 Pin Assignments

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

1.5.8 Pin Assignments for the MDI/MDI-X Port Configuration

The EH switches support auto MDI/MDI-X (Medium-Dependent Interface/ Medium Dependent Interface-Automatic Crossover) port configuration; one may use a straight-through UTP-RJ-45 cable to connect a PC to the EH switch. The following table shows the pin assignments for the connector.

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

Note: **"+" and "-" signs represent the polarity of the wires that make up the wire pairs.**

1.5.9 Optical-Fiber and Connector Types

All fiber channels are designated for transmission at Gigabit speed. There are two models: EH 6508G-Fm and EH 6508G-Fs.

The EH6508G-Fm Model is equipped with multi-mode fiber (50/125 μm or 62.5/125 μm core/cladding type) SC connectors. The wavelength is short IR @ 850 μm. The EH6508G-Fm Model has a maximum transmission distance of 550m while using 50/125 μm cabling.

The EH6508G-Fs Model is equipped with two single mode fiber channels (10/125 μm core/cladding type), and is designated for transmitting gigabit rate up to 5 km distance.

The user should note that the TX port of Switch A should be connected to the RX port of Switch B and vice versa.

Part 2 Configuring with a Web Browser

2.1 Web-based Management Basics

There is an embedded HTML web site in the flash memory on the switch's CPU board. This embedded site allows a user to manage the switch remotely through a standard browser like **Microsoft Internet Explorer**.

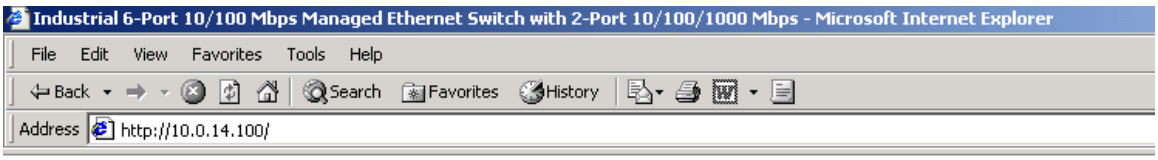
The Web-Based Management tool supports Internet Explorer 5.0 or its later version. If the user has an IE5.0 or the older versions he/she must first enable the Java Applets before use.

2.2 Defauts

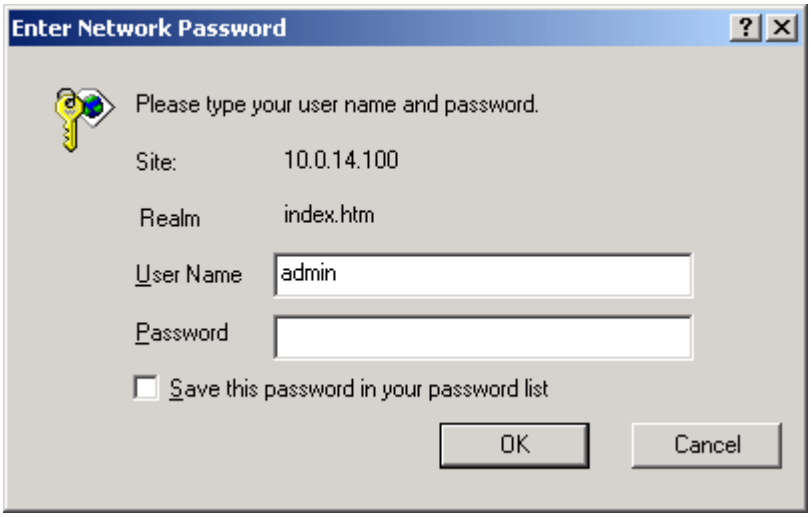
The default values for a switch are:

IP Address: 10.0.50.100
Subnet Mask: 255.255.0.0
Default Gateway: 10.0.0.254
User Name: **admin**
Password: Press "Enter"

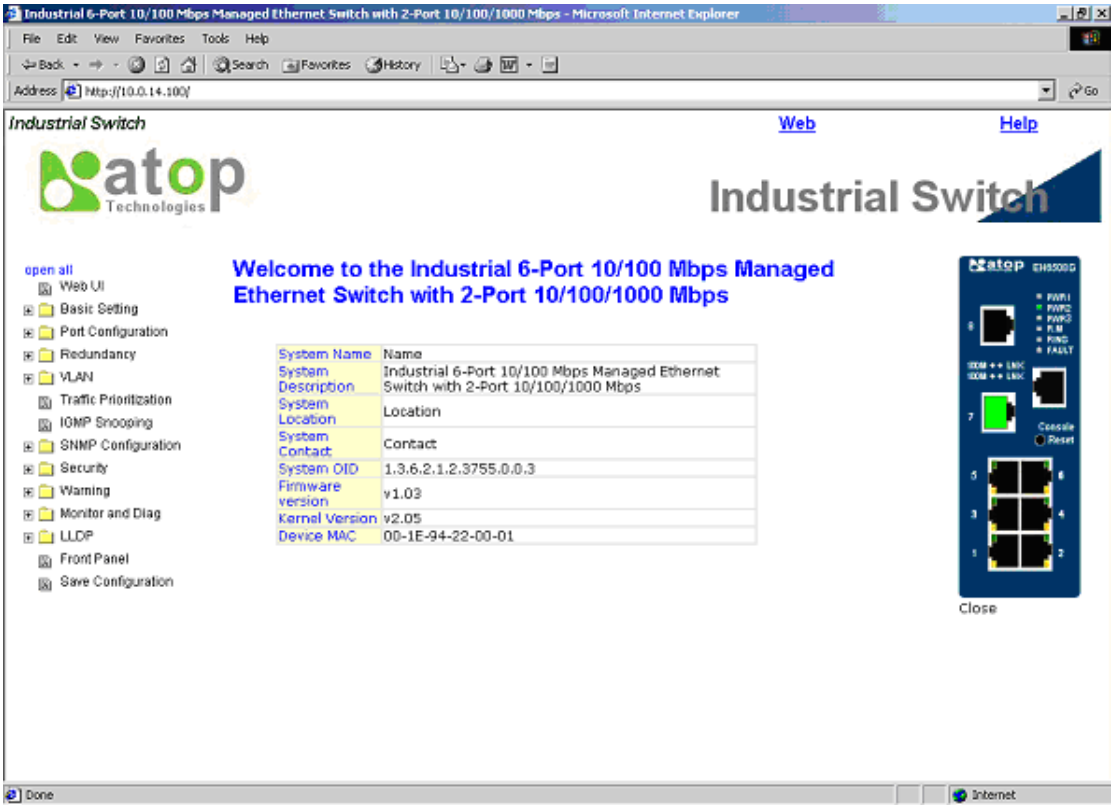
2.3 Login and Main Window Interfaces


Industrial 6-Port 10/100 Mbps Managed Ethernet Switch with 2-Port 10/100/1000 Mbps - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://10.0.14.100/

1. Launch the Internet Explorer
2. Type http:// and the IP address of the switch, then "**Enter**"
3. The login screen shall appear
4. Key in the username (default: admin) and password (default: blank)
5. Click "**Enter**" or "**OK**" button, then the Main Interface Window shall appear (see below)



Login screen

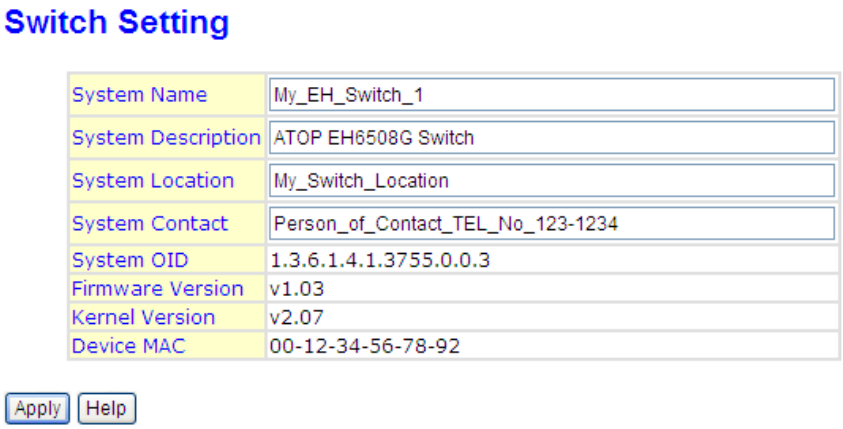

Industrial 6-Port 10/100 Mbps Managed Ethernet Switch with 2-Port 10/100/1000 Mbps - Microsoft Internet Explorer
Industrial Switch
Web
Help
Industrial Switch
Welcome to the Industrial 6-Port 10/100 Mbps Managed Ethernet Switch with 2-Port 10/100/1000 Mbps
System Name Name
System Description Industrial 6-Port 10/100 Mbps Managed Ethernet Switch with 2-Port 10/100/1000 Mbps
System Location Location
System Contact Contact
System OID 1.3.6.2.1.2.3755.0.0.3
Firmware version v1.03
Kernel Version v2.05
Device MAC 00-1E-94-22-00-01
Close

Main interface

2.4 Basic Settings

The following sections describe the parameters on the left hand side of the main window.

2.4.1 SWITCH SETTING

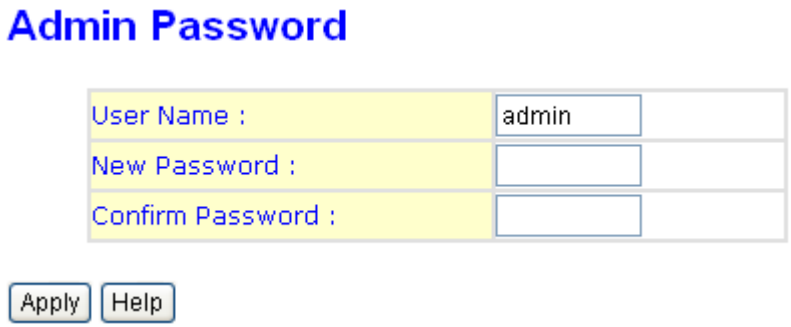


Switch setting interface

Label	Description
System Name	Enter the name of switch. The maximum length is 64 bytes.
System Description	Enter the description of switch.
System Location	Enter the switch physical location. The maximum length is 64 bytes.
System Contact	Enter the name of contact person.
System OID	Object ID (furnished by Atop)
Firmware Version	Switch's firmware version (furnished by Atop)
Kernel Version	Kernel software version (furnished)
Device MAC	The unique hardware MAC address (furnished)

2.4.2 ADMIN AND PASSWORD

One can then proceed to change login **User Name** and the **Password**.



Admin Password interface

Label	Description
User name	Key in the new **User Name** (The default is "admin").
New Password	Key in the new **Password** (The default is " enter", or blank).
Confirm password	Re-type the new **Password.**
Apply	Click **Apply** to confirm the changes; Select "**File->Save**" to save the setup.

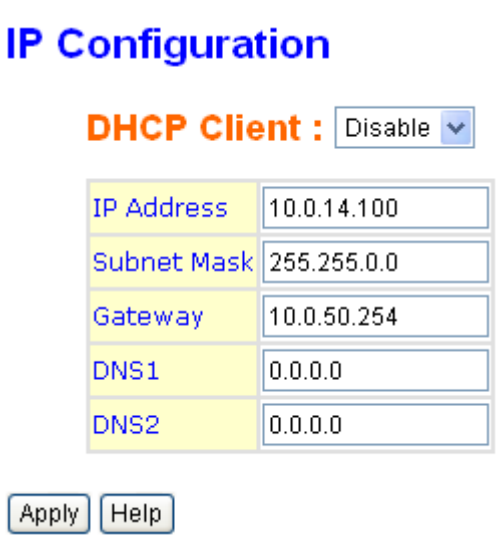
2.4.3 IP CONFIGURATION

The Switch is furnished with a factory default IP address 10.0.50.100.

It is important to make sure that before plugging in the switch onto the LAN the IP 10.0.50.100 has not been assigned, otherwise the switch may not be “discovered” because of IP conflicts. Likewise, if two EH switches are installed on the same LAN, the identical IPs of 10.0.50.100 also will cause conflict. In this case, the user may use “IP Configuration” to change the switch’s IP from the default value.

To do so, the user is recommended to disconnect the switch and the host from the LAN, and enter the default IP 10.0.50.100 to “discover” the switch. After the “Welcome” page, go to “Basic Setting-> IP Configuration”, and select to “disable” the “DHCP Client” mode. Go ahead and change the “IP Address”. In the following example, the switch IP has been changed to 10.0.14.100.

It should noted that the new IP Configuration is “applied” to the current session by clicking on “Apply” button. To save the new new IP configuration, one must also press “File->Save” to save into the flash memory.



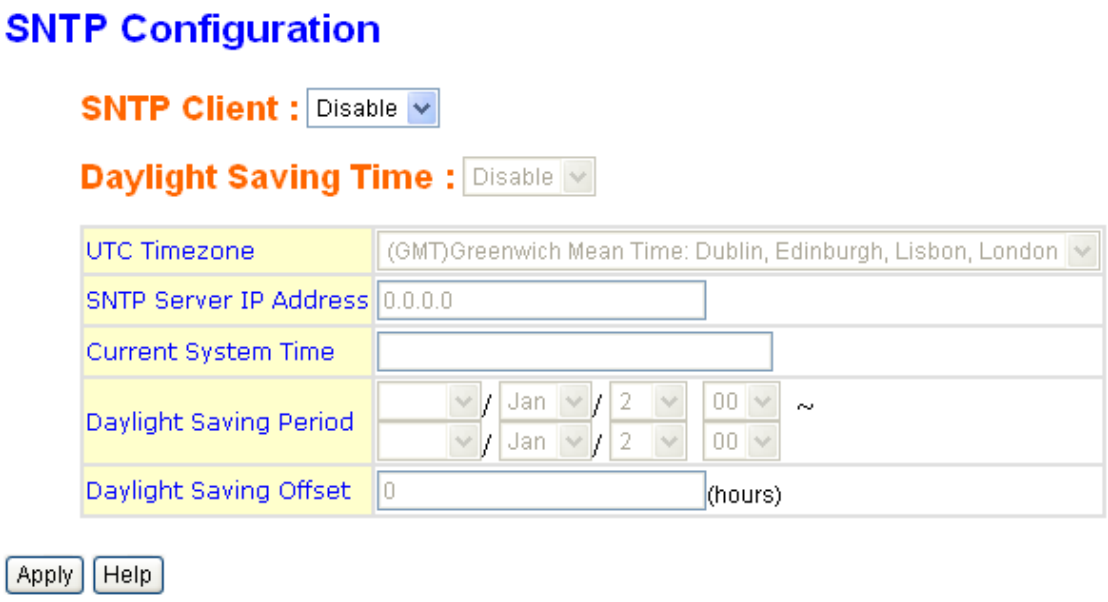
If “DHCP Client” is in “Enable”, the switch IP will be assigned by the DHCP server on the LAN, which is not normally done. As expected, “DHCP Client” is enabled, there is no need for any entry (see below).

2.4.4 TIME (SNTP) AND TIME ZONES OF THE WORLD

The user can synchronize the switch time with a chosen SNTP server (SNTP: Simple Network Time Protocol). If **SNTP Client** is enabled, the switch clock is synchronized with the SNTP server clock, otherwise (shown in the diagram below) the switch time is not a "client" of the SNTP server.

A SNTP server can found on the Internet (http://support.microsoft.com/kb/262680). For instance the Hong Kong server is at 137.189.6.18.

If the switch is the client of a SNTP server, then one needs enter the SNTP server address and decides if the Daylight Saving Time should be selected.


SNTP Configuration
SNTP Client : Disable
Daylight Saving Time : Disable
UTC Timezone (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
SNTP Server IP Address 0.0.0.0
Current System Time
Daylight Saving Period / Jan / 2 00 ~
/ Jan / 2 00
Daylight Saving Offset 0 (hours)
Apply
Help

SNTP Configuration interface

AS a reference, the time zone of the world is attached here.

Time zones of the World

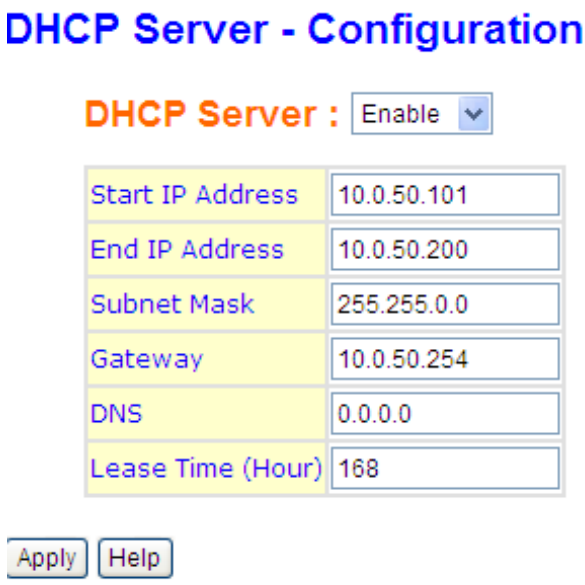
Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, USSR Zone 1	+2 hours	2 pm
BT - Baghdad, USSR Zone 2	+3 hours	3 pm
ZP4 - USSR Zone 3	+4 hours	4 pm
ZP5 - USSR Zone 4	+5 hours	5 pm
ZP6 - USSR Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, USSR Zone 7	+8 hours	8 pm

JST - Japan Standard, USSR Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, USSR Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

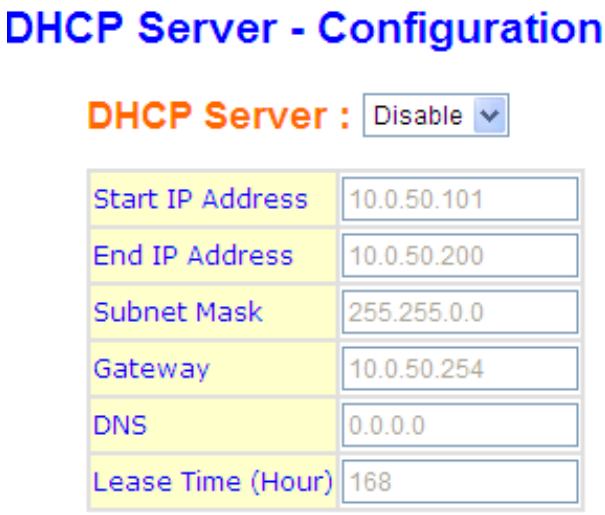
2.4.5 SWITCH AS A DHCP SERVER

2.4.5.1 Configuration (to be a DHCP Server)

The switch can be assigned to be a DHCP (Dynamic Host Configuration Protocol) server by setting the **DHCP Server** function in “enable”.



Otherwise, if in “disable”, there is no need to define any entry.



If switch's DHCP server function is enabled, then one must fill out the "**Start IP Address**" and the "**End IP Address**". For instance, if the assigned dynamic IP range is from 10.0.1.100 ~ 10.0.1.200, then 10.0.1.100 is the **Start IP Address**, and 10.0.1.200 will be the "**End IP address**". A typical **Subnet Mask** is "255.255.0.0". An example **Gateway** IP is: 10.0.50.254. Normally, there is no need for assigning the DNS IP in a LAN environment unless the LAN is hooked up to the Internet, then the DNS is your ISP DNS server IP. InTaiwan, the **Hinet** DNS server is 168.95.1.1. "Lease Time" is expressed in hours, which spells out the time when the DHCP IP shall remain unchanged (in case another DHCP is accidentally assigned to be the DHCP server of the LAN.)

Before enabling the DHCP server function, make sure there is no existing DHCP server on the LAN otherwise the system can be confused as to which server the client should "listen to". Also, serving as the DHCP server adds to the work load of the switch so other tasks may be slowing down because of the added role.

2.4.5.2 Client Entries (of a DHCP server)

When the DHCP server function is enabled on the switch, the switch will collect all the DHCP Client information and display here. The example shows a Client Entry of 10.0.51.101 being collected.

DHCP Server - Client Entries

IP Address	MAC Address	Type	Status	Lease
10.0.50.101	00:18:DE:02:92:73	dynamic	DHCP	604518

2.4.5.3 Port and IP Binding

The user can assign (hence "bind") a specific **IP Address** (within the assigned IP range) to a specific port on a switch. Once a port is connected and queries for a dynamic IP assignment, it will receive the IP assigned in this Table by the switch. This "binding" is possible only when the switch is enabled to be the DHCP server, otherwise thee is no entry. In the example below, Port 5 is "bound" to IP:10.0.51.100.

DHCP Server - Port and IP Binding

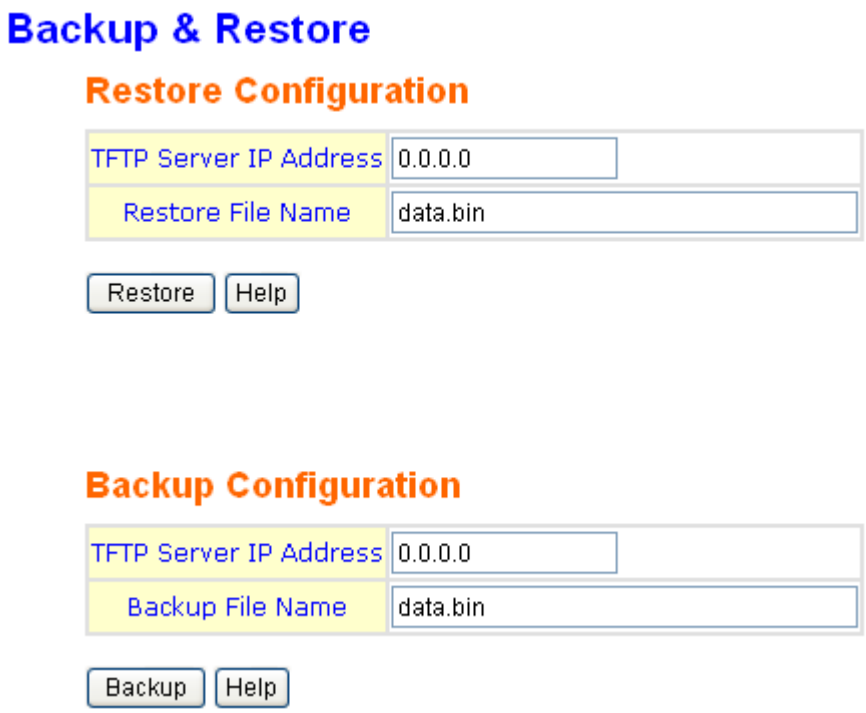
Port No.	IP Address
Port.01	0.0.0.0
Port.02	0.0.0.0
Port.03	0.0.0.0
Port.04	0.0.0.0
Port.05	10.0.51.100
Port.06	0.0.0.0
G1	0.0.0.0
G2	0.0.0.0

Apply Help

DHCP Server Port and IP Binding Interface

2.4.6 BACKUP & RESTORE

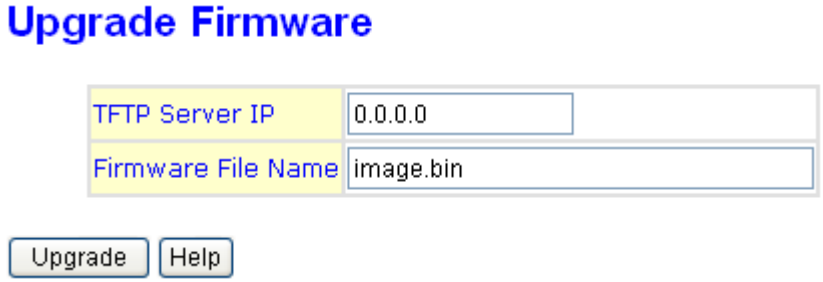
Backup function allows the user to save current configuration from the switch EEPROM onto the **TFTP** (Trivial File Transport Protocol) server, while the **Restore** function sends a saved configuration file (.bin) to the EEPROM of a switch. One may obtain a TFTP server program on the Web (example site: http://tftpd32.jounin.net/)



Restore & Backup Interfaces

2.4.7 UPGRADE FIRMWARE

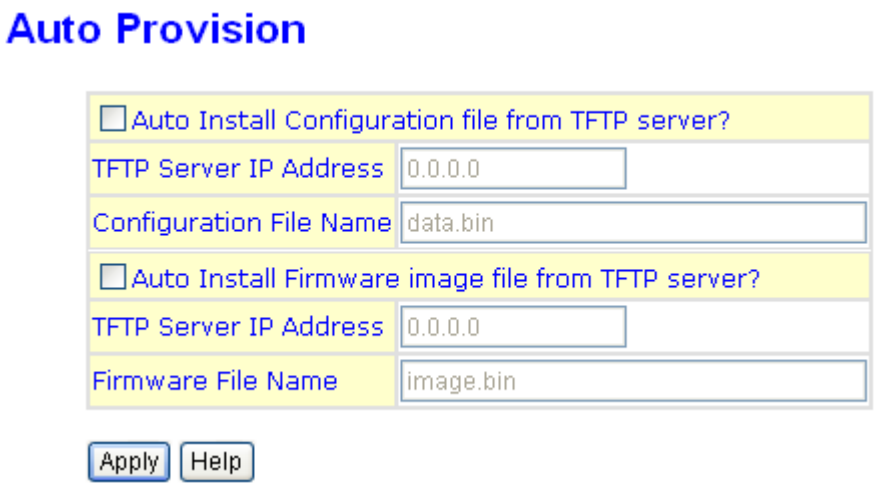
This allows the user to update the switch firmware. Before doing so, make sure to have the TFTP server ready and the new firmware image on the TFTP server.



Update Firmware **interface**

2.4.8 AUTO PROVISION (AUTO-UPDATING)

This allows the user to update the switch firmware automatically. The user can store the new firmware (the configuration file) on the TFTP server, then when the user reboots the switch, updating takes place automatically.



Auto Provision interface

2.4.9 FACTORY DEFAULT

Factory Default interface

The Factory Default function allows the user to reset the switch to the factory default state or to reset the switch **unless the**

"Keep current IP address setting" or the

"Current username and password" box is checked.

2.4.10 SYSTEM REBOOT

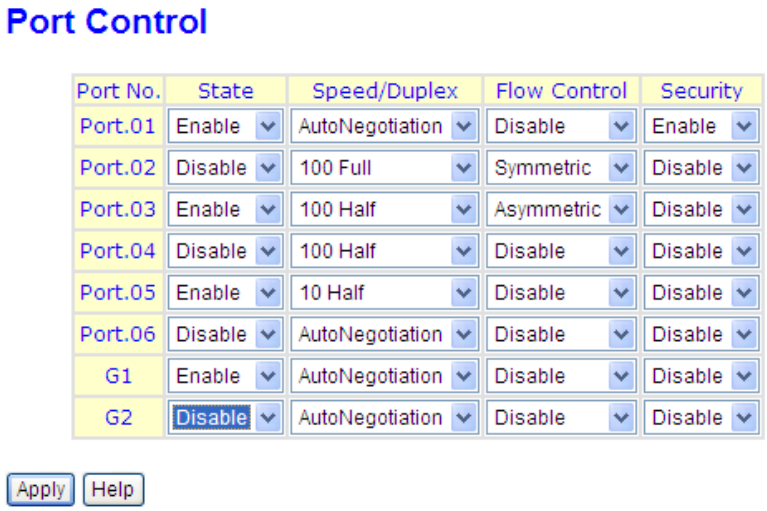
This function allows the user to reboot the switch by clicking "**Reboot**".

System Reboot **interface**

2.5 Port Configuration

2.5.1 PORT CONTROL

This function allows the user to set **state (enable or disable), speed/duplex, flow control,** and **security** of each port.


Port Control
Port No. State Speed/Duplex Flow Control Security
Port.01 Enable AutoNegotiation Disable Enable
Port.02 Disable 100 Full Symmetric Disable
Port.03 Enable 100 Half Asymmetric Disable
Port.04 Disable 100 Half Disable Disable
Port.05 Enable 10 Half Disable Disable
Port.06 Disable AutoNegotiation Disable Disable
G1 Enable AutoNegotiation Disable Disable
G2 Disable AutoNegotiation Disable Disable
Apply
Help

Port Control **interface**

Label	Description
Port NO.	Port number on the switch.
Speed/Duplex	Select either **AutoNegotiation**, **100 full, 100 half, 10 full or10 half-duplex** mode of transmission.
Flow Control	Either enable or disable "**Flow Control**" to avoid packet loss when congestion occurs. If enabled, select "**Symmetric**" or **Asymmetric"**.
Security	Enabling the **Security** function will stop unauthorized hosts from accessing the port. **See 2.11.2 Port Security.**
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.

2.5.2 PORT STATUS

The function provides the port status on **Type** (10, 100, or 1000 Mbps), **Link** condition (up or down)**, State** (enabled or disabled), **Speed/Duplex and Flow Control**.

Port Status

Port No.	Type	Link	State	Speed/Duplex	Flow Control
Port.01	100TX	Down	Enable	N/A	N/A
Port.02	100TX	Down	Enable	N/A	N/A
Port.03	100TX	Down	Enable	N/A	N/A
Port.04	100TX	Down	Enable	N/A	N/A
Port.05	100TX	Down	Enable	N/A	N/A
Port.06	100TX	Down	Enable	N/A	N/A
G1	1000TX	UP	Enable	100 Full	Disable
G2	1000TX	Down	Enable	N/A	N/A

Port Status Interface

2.5.3 RATE LIMIT

The **Rate Limit** function sets limits on the incoming transmission ("**Ingress"**) types for a given port; include **broadcast, multicast, flooded Unicast**, and by its transmission rate for the incoming ("**ingress**") and the out-going ("**egress**") traffics.

Rate Limiting

	Ingress Limit Frame Type	Ingress	Egress
Port.01	Broadcast only	8192 kbps	0 kbps
Port.02	Broadcast only	8192 kbps	0 kbps
Port.03	Broadcast only	8192 kbps	0 kbps
Port.04	Broadcast only	8192 kbps	0 kbps
Port.05	Broadcast only	8192 kbps	0 kbps
Port.06	Broadcast only	8192 kbps	0 kbps
G1	Broadcast only	8192 kbps	0 kbps
G2	Broadcast only	8192 kbps	0 kbps

Rate range is from 100 kbps to 102400 kbps (i.e. 100Mbps) for mega-ports, or 256000 kbps (i.e. 250Mbps) for giga-ports. Zero means no limit.

Apply Help

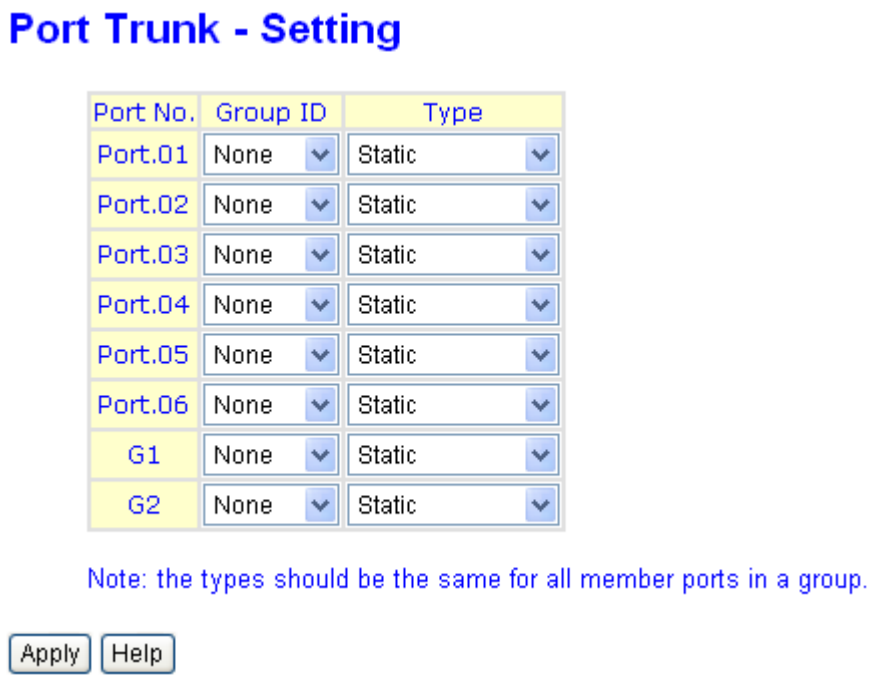
Rate Limit interface

Label	Description
Ingress Limit Frame Type	The user can choose among: "**all**", **"Broadcast only" , "Broadcast/Multicast" or "Broadcast/Multicast/Flooded Unicast"** mode.
Ingress	Receiving data rate. "**0**" implying "**Auto Negotiation**" or "**no limit is placed**". "0" is the default value.
Egress	Outgoing data rate. "**0**" implies "**Auto Negotiation**" or "**no limit is placed**". **"0"** is the default value.
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.

2.5.4.1 Port Trunk Setting

2.5.4 PORT TRUNK

The user can select **static** trunk or **802.3ad LACP link aggregation** to increase bandwidth by combining several physical links into a logical link.



Label	Description
Group ID	The trunk number which the port belongs to (trunk 1 to trunk 4).
Type	**Static** trunk or **802.3ad LACP link aggregation**
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.

Port Trunk—Setting **interface**

2.5.4.2 Port Trunk Status

Port Trunk - Status

Group ID	Trunk Member	Type
Trunk 1		Static
Trunk 2		Static
Trunk 3		Static
Trunk 4		Static

Port Trunk—Status interface

If, say, we group ports 1, 2 and 3 into **trunk 1**, then enter 1,2,3 under “Trunk Member”.

2.6 Redundancy

2.6.1 iA -Ring, Coupling Ring and Dual Homing Ring

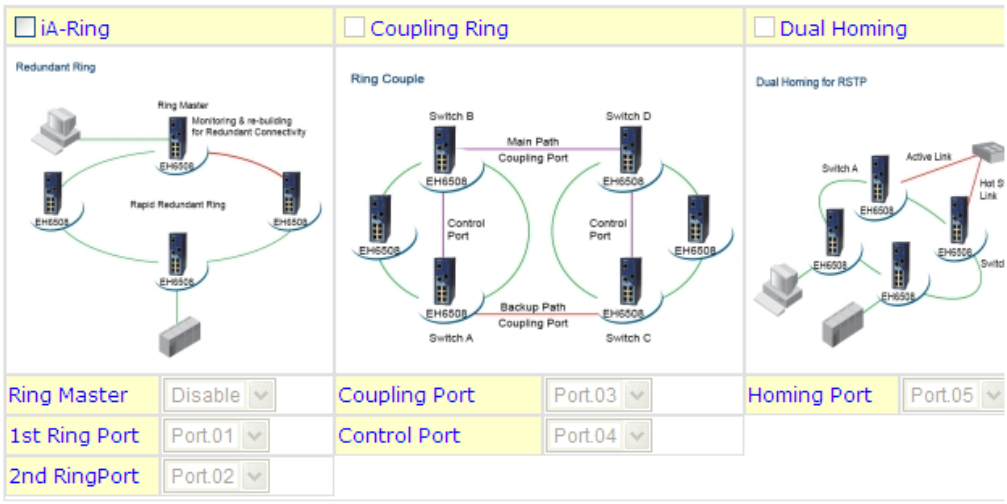
An iA Ring falls into the category of Rapid R Rings, but with its own protocols. Atops’ iA Ring has a unique feature of reducing network breakage recovery time to 10 ms or less. The EH series supports ring topology with ready redundancy and fast recovery time in case of ring breakage. An IA-Ring can form a stand-along ring, or join two rings to form a Coupling Ring in which if the topology is changed, the other ring will not be affected. In the situation when an external server (RSTP server) needs redundancy, it can be hooked up to two switches in an iA Ring to form a “**Dual Homing**” configuration.

A Coupling Ring requires at least four switches to form a ring with an active link and a backup link.

To use iA Ring, first check “iA Ring. If any of the following two topologies is used, then check the individual box on the upper box, or both if needed. The Coupling Ring is formed by joining two iA Rings with redundant paths. As shown below, two iA rings are “coupled” at Switches B--D and A—C, so either path can be the main path while the other serves as a redundancy. In the case when extra redundancy is imperative, extra “control ports” can be connected as shown in the following diagram where Control Ports between switches A—B and switches C—D are connected to double its redundancy to avoid network down time, Control signals are transmitted between the Control ports between switches A—B and switches C—D.

When an additional server (a RSTP server shown in the diagram) is attached to the iA Ring, then a “Dual Homing” configuration is desirable for redundancy. This is shown below under “Dual Homing”.

It is highly recommended that a user completes configuration of individual switches before making physical connection to avoid unexpected looping.



Label	Description
IA-Ring	Check the box to enable **IA-Ring**.
Ring Master	There should be only one **Ring Master** in a ring. However if two or more Ring Masters happen to be assigned, the one with the lowest **MAC address** will act the de-facto **Ring Master** and others is the **Backup Master**.
1st Ring Port	The primary port o the Ring Master port
2nd Ring Port	The backup port if this switch is the Ring Master.
Coupling Ring	After "iA-ring is selected, check "Coupling Ring" box to enable the Coupling Ring. Click on a given switch (A,B,C,or D) and define the Coupling Port no. or the Control Port no. as shown below .
Coupling Port	The port number where two rings are joined
Control Port	The port number where the Control line is connected.
Dual Homing	Check the "Dual Homing" box to enable Dual Homing topology. Click on one of the two switches (A or B) that serve as two "homing paths" and define each "Homing Port" as shown below.
Homing Port (Dual Homing)	The **Homing port IP** where the two links work as active/backup link.
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.

[Note]: We do not recommend the user to set one switch as a Ring Master and a Coupling Ring at the same time; it will place heavy loading on the switch.

2.6.2 RSTP

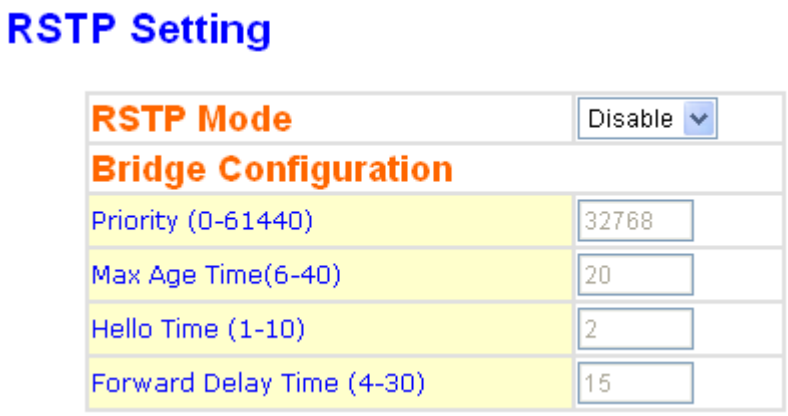
In a complex network, the EH series switches can serve as the “bridges” which function as the “nodes”. Between the nodes are the network “segments”. It is essential that the network operation does NOT run in an endless loop where a packet of information continuously wanders in a loop and cannot be directed to the correct node. Hence “Spanning Tree Protocol” was created and a set of agreed rules are followed for all bridges to collectively compute a “spanning tree”. Once a spanning tree is established, then there shall be no loops in a network.

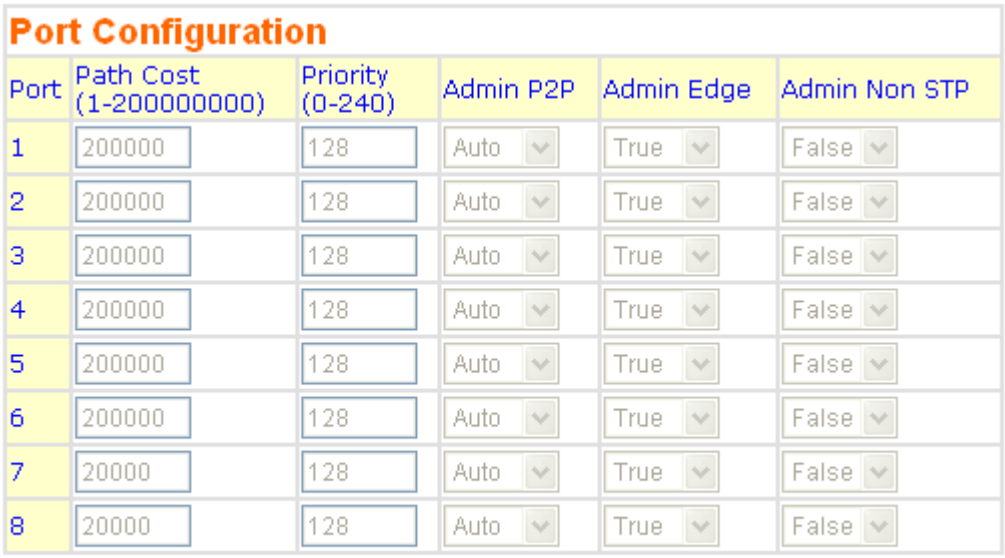
Likewise, when the tree is disturbed from partial breakage of the network, the protocol computes a new tree.

The Rapid Spanning Tree Protocol (**RSTP**) is an improved version of the Spanning Tree Protocol (**STP**) which is slow in convergence. RSTP also has a faster convergence (than the STP does) when a network topology changes, for instance, a new switch is inserted. It was released in 1998 by **IEEE**, known as **802.1w.**

2.6.2.1 RSTP Setting

There the user can enable/disable the RSTP function, and set parameters for each port.





RSTP Setting interface

Label	Description
RSTP mode	Before configuring the rest of the parameters, the **RSTP** mode must be in “enable”.
Priority (0-61440)	A value between 0 and 61440 and a multiple of 4096 is used to identify the root bridge. The bridge with the lowest value has the highest priority and is “selected” as the root. If the value changes, the switch must be rebooted.
Max Age (6-40)	The number of seconds a bridge waits without receiving Spanning-tree Protocol configuration messages before attempting a reconfiguration.
Hello Time (1-10)	The number in seconds that a switch sends out the BPDU packets to check RSTP status.
Forwarding Delay Time (4-30)	The number in seconds a port waits before changing from its RSTP learning and listening states to forwarding state.
Path Cost (1-200000000)	The “cost” of the path to the other bridge from this source bridge port to the specified destination port. Enter a number 1 through 200,000,000. The path between two switches or bridges adds the “cost” by one.
Priority (0-240)	A multiple of 16, between 0 and 240, assigned for a port to be the blocking port in a network. The lower the number, the less likely to be blocking.
Admin P2P	This function allows the P2P status of the link to be

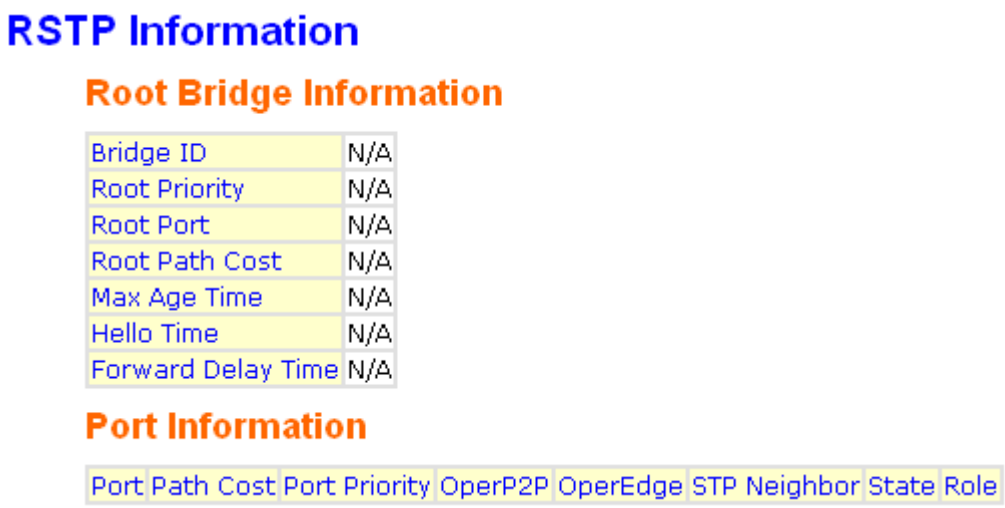
	manipulated administratively: “True” to enable P2P; “False” to disable.
Admin Edge	To configure a port to be an **edge** port, check “**True**”.
Admin Non STP	Select “**True”** to **Exclude** a port from the STP mathematic calculation, select “**False”** to include the port in the STP mathematic calculation.
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.

[NOTE] **Follow the following formula to configure MAX Age, Hello Time, and Forward Delay Time.**

2 x (Forward Delay Time value –1) > = Max Age >= 2 x (Hello Time +1)

2.6.2.2 RSTP Information

RSTP Information displays the configured RSTP status.



RSTP Information interface

2.7 VLAN

A virtual LAN, or VLAN, is a network with various hosts of a common set of requirements. These hosts, thus switches, function as if they were physically connected as a LAN. A VLAN has all the same attributes as a physical LAN, but it allows for “edge stations” (end stations) to be grouped together even if these edge stations are not located on the same LAN segment. Network reconfiguration is performed entirely through software instead of physically relocating devices.

Virtual LAN limits the broadcast to within the LAN domain; hence it allows the user to isolate

network traffic, and only members receive traffic from the other members of the same VLAN. The EH switches support both **Tagging-based (802.1Q)** VLANs and **Port-based** VLANs. The default mode is "**Tagging-based** or **802.1Q**".

Note that special Network Interface Cards (NIC) that support VLAN protocol must be used for such task.

2.7.1 TAGGING-BASED VLAN – 802.1Q

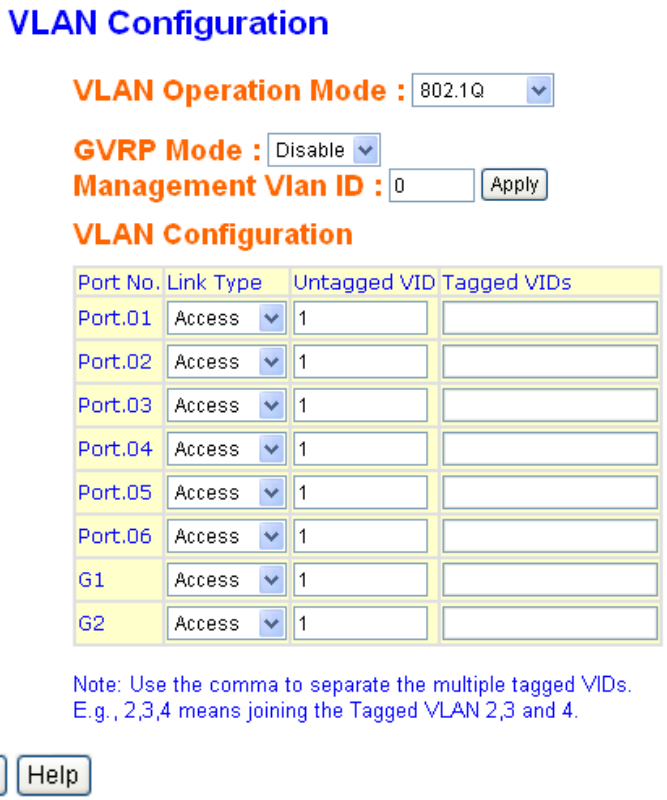
The Tagging-based VLAN follows **IEEE 802.1Q** (known as VLAN Tagging) specification standard. Therefore, it is possible to create a VLAN with devices from different switch venders. **IEEE 802.1Q** VLAN inserts a "tag" onto the Ethernet frames, which contains a VLAN Identifier (**VID**).

With the EH series, the user can create a Tagging-based VLAN, enable or disable **GVRP** protocol. There are 256 VLAN groups possible. Enabling **802.1Q** VLAN forces the all ports on the switch to the default untagged VID of 1 if there is only one switch (**Access** Link). Since by default all port within a switch can "talk: to each other and hence they form a default VLAN and the default VLAN can't be removed.

For a VLAN involving two or more switches, **802.1Q Link** (Shown in the diagram as "**1QTrunk**") allows the same "**Tagged VID**" to be assigned, and hence the user must enter the **"Tagged VIDs"** value (between 0 and 4094). For VLANs that require high transmission connection to the backbone typically take advantage of the Giga ports on the switch.

If "**Hybrid** Link" is chosen, then both **Untagged VID** and **Tagged VIDs** are open for inputs (between 0 and 4094).

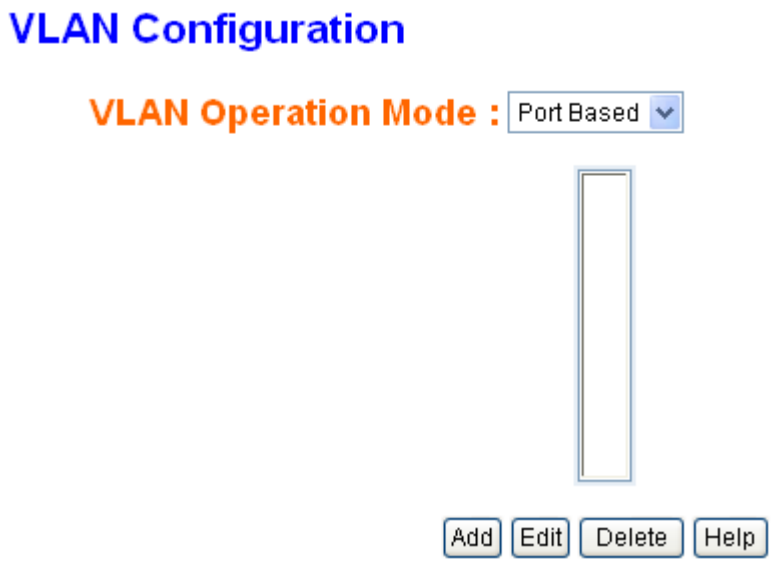
GVRP(Generic VLAN Registration Protocol) allows automatic VLAN configuration between the switch and nodes (PC's, servers, printers, etc). If the switch is connected to a device with **GVRP** enabled, the user can send a **GVRP** request using **VID** on a **VLAN**; the switch will automatically add that device to the existing **VLAN**.


VLAN Configuration
VLAN Operation Mode : 802.1Q
GVRP Mode : Disable
Management Vlan ID : 0 Apply
VLAN Configuration
Port No. Link Type Untagged VID Tagged VIDs
Port.01 Access 1
Port.02 Access 1
Port.03 Access 1
Port.04 Access 1
Port.05 Access 1
Port.06 Access 1
G1 Access 1
G2 Access 1
Note: Use the comma to separate the multiple tagged VIDs.
E.g., 2,3,4 means joining the Tagged VLAN 2,3 and 4.
Apply Help

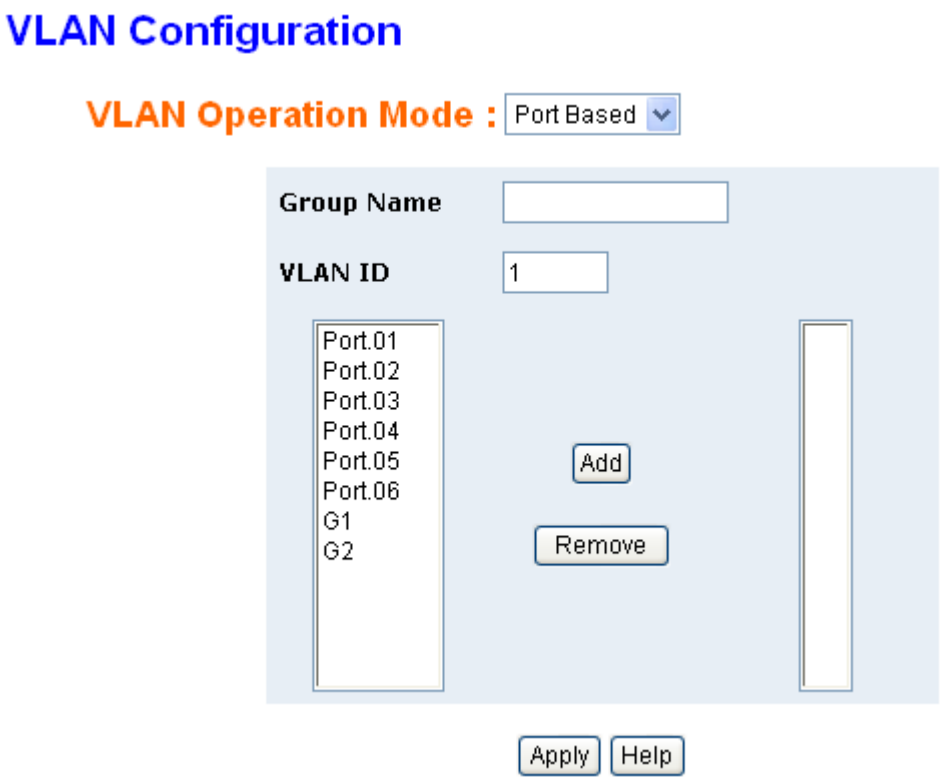
Label	Description
VLAN Operation Mode	Select a **VLAN** Operation Mode among :**Disable, Port-based, or 802.1Q (tagging-based)**
GVRP Mode	"Enable/Disable" GVRP function.
Management VLAN ID	Assigning the **VLAN** ID; only the devices within the "Management **VLAN** ID can access the network.
Link type	Select one from the 3 link types: **Access:** for single switch only; allows the user to group ports by setting the same **Untagged VID** **802.1Trunk:** an extended application of **Access** Link, allows the user to group ports by setting the same **Tagged VID's** for 2 or more switches. **Hybrid:** Both **Access** Link and **Trunk** Link are available.
Untagged VID	Enter the default **VLAN** ID for untagged devices connected to the port. The range is 1 ~ 4094.
Tagged VIDs	Enter the tagged VIDs to carry different **VLAN** frames to other switch(s).
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.

2.7.2 PORT-BASED VLAN

In a Port-based VLAN, packets can only go among members of the same **VLAN** group. Once Port-based VLAN is selected, click "Add" to include ports from the switch to be members for the VLAN. A "Group Name" must be filled out. If the VLAN ID is 2, and the "Group name is "Mygroup" then the VLAN's full name is "Mygroup_2". Note all unselected ports are treated as belonging to the default **VLAN** because they can still communicate among themselves. There can be more than one VLANs assigned to one switch port. Use "Edit" to edit an existing VLAN. While in "Edit", use "Add" and "Remove" for port addition and deletion.



Label	Description
Add	Enter **VLAN** "**Add**" interface.
Edit	Edit existing **VLAN**.
Delete	Delete existing **VLAN**.
Help	**Display "Help" file.**



Port-based VLAN interface

Label	Description
Group Name	Enter **VLAN** name.
VLAN ID	Enter **VLAN** ID.
Add	Add port to the **VLAN**.
Remove	Remove port from the **VLAN**
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.
Help	**Display "Help" file.**

2.8 Traffic Prioritization

Traffic Prioritization can be defined by three methods: **Port-based, 802.1p/COS** (**COS**: class of service), and **TOS/DSCP** (**TOS**: Type of Service; **DSCP**: Differentiated Services Code Point) With **Traffic Prioritization** function, the user assigns data traffic into four classes (**High, Middle, Low** and **Lowest**) for differentiate network applications.

Traffic Prioritization

Qos Policy :

- (•) Use an 8,4,2,1 weighted fair queuing scheme
- ( ) Use a strict priority scheme

Priority Type : Disable

Apply | Help

Port-based Priority :

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	G1	G2
Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest

Apply

COS/802.1p :

	0	1	2	3	4	5	6	7
Priority	Low	Lowest	Lowest	Low	Middle	Middle	High	High

COS Port Default :

Port.01	Port.02	Port.03	Port.04	Port.05	Port.06	G1	G2
0	0	0	0	0	0	0	0

Apply

TOS/DSCP :

DSCP	0	1	2	3	4	5	6	7
Priority	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
DSCP	8	9	10	11	12	13	14	15
Priority	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest	Lowest
DSCP	16	17	18	19	20	21	22	23
Priority	Low	Low	Low	Low	Low	Low	Low	Low
DSCP	24	25	26	27	28	29	30	31
Priority	Low	Low	Low	Low	Low	Low	Low	Low
DSCP	32	33	34	35	36	37	38	39
Priority	Middle	Middle	Middle	Middle	Middle	Middle	Middle	Middle
DSCP	40	41	42	43	44	45	46	47
Priority	Middle	Middle	Middle	Middle	Middle	Middle	Middle	Middle
DSCP	48	49	50	51	52	53	54	55
Priority	High	High	High	High	High	High	High	High
DSCP	56	57	58	59	60	61	62	63
Priority	High	High	High	High	High	High	High	High

Apply

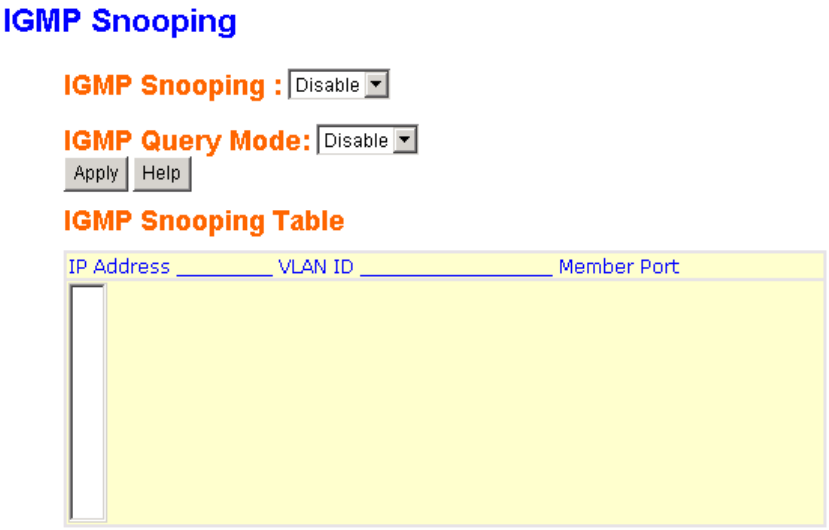
Traffic Prioritization interface

Label	Description
QoS policy	**If "Use an 8,4,2,1 weighted-fair- queue scheme"** is checked, output queues follow the 8:4:2:1 ratio for transmitting packets for "high, middle, low, lowest" priorities. For example: 8 "high" queue packets, 4 "middle" queue packets, 2 "low" queue packets, and one "lowest" queue packet are transmitted in one frame. **If "Use a strict priority scheme"** is checked, then always the packets of high priority queues are transmitted first, followed by middle, low, and lowest (priority) queues.

Priority Type	**Port-base:** output priority is determined by priority assigned to the ingress port. **COS only:** output priority is determined by **COS** only. **TOS only:** output priority is determined by **TOS** only. **COS first:** output priority is determined first by **COS** then by **TOS** **TOS first:** output priority is first determined by **COS** then by **TOS**
Port-based Priority	Assign each Port with a priority: **High, Middle, Low, and Lowest.**
COS/802.1p	**COS** (Class Of Service) is well known as 802.1p: output priority is determined by the user priority field in 802.1Q **VLAN** tag. The priority value maps 0~7.COS value to 4 priority queues: **High, Middle, Low, and Lowest.**
COS Port Default	When an ingress packet has not **VLAN** tag, a default priority value is determined by the ingress port.
TOS/DSCP	**TOS** (Type of Service) is a field in the IP header, which is also used in **DSCP**. The output priority can be divided into to 0~63. The 64 **DSCP** priority values can be mapped to 4 priorities: **High, Middle, Low, and Lowest**.
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.
Help	**Display "Help" file.**

2.9 IGMP Snooping

Internet Group Management Protocol (**IGMP** v1, v2 and v3 (**RFC 1112, 2236 and 3376**) is used by the IP hosts to register their dynamic multicast group membership. IGMP Snooping, when enabled on an EH switch, will "snoop" traffic on a switch, and the switch will inspect the IGMP messages passing between a host and a router, and add the necessary ports to its multicast table, ensuring that only the ports that require a given multicast stream actually receive it. IGMP improves the network performance by reducing LAN traffic congestion. Note that multicast group addresses are IP addresses between 224.0.0.0 and 239.255.255.255.



IGMP Snooping **interface**

Label	Description
IGMP Snooping	Enable/Disable IGMP snooping.
IGMP Query Mode	If in "enable", the switch is the IGMP querier. "Auto" means that the querier is automatically assigned to the one with the lowest IP.
IGMP Snooping Table	Display current IP multicast list.
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.
Help	**Display "Help" file.**

2.10 SNMP Configuration

Simple Network Management Protocol (**SNMP**) is a protocol developed to manage nodes (servers, workstations, routers, switches and hubs etc.) on an IP network. **SNMP** enables network administrators to manage network performance, to find and solve network problems, and to plan for network growth. Network management systems learn problems by receiving traps or change notices from network devices implementing **SNMP**. One may download an SNMP MIB (Management Information Base) Browser from the Internet (Example site: http://www.ireasoning.com/) for viewing the information. Note that V1 and V2 are usually provided for free of charge, but V3 package is not, and must be purchased.

2.10.1 SNMP–AGENT VERSIONS (V1/V2 OR V3)

The user can set **SNMP** agent related information via **SNMP Agent Setting** function.

Three **SNMP** versions are supported here: V1/ V2c in one group, and V3 in another. **V1/V2c agent** uses community string match for authentication with either **read-only** or **read-and-write** privilege. **SNMP**V3 agent requires an authentication level of MD5 or DES to encrypt data to enhance data security.

SNMP- Agent Setting interface

Label	Description
SNMP agent Version	Select **SNMPV1/ V2c**, or **SNMPV3**.
SNMP V1/V2c Community	If **SNMP V1/V2c Agent Version** is checked, one may proceed to define up to four Community groups, with a maximum 32 characters. On the right, select between "**Ready Only**" or "**Read and Write**" privilege.
SNMPv3User	If **SNMP V3 agent** is selected, then at least one **SNMPv3 User** profile must be created. **Auth Password** is encrypted in MD5 and **Privacy Password**, which is encrypted in DES, need not to be identical to **Auth Password**. There are maximum 8 sets of **SNMP**v3 users and a maximum 16 characters in username, and password fields. Check "**Remove**" to remove a current user profile. To do so, you must type in the User name, Auth Password, and Privacy Password before clicking "Remove"
Current SNMPv3 User Profile	Display all **SNMP**v3 user profiles.
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.
Help	Display **Help** file.

2.10.2 SNMP –TRAP SETTING

A trap manager is a management station that receives system alerts generated by the switch. These alerts are called "traps" (after Version 1, traps are called "Notifications). If no trap manager is defined, no traps will be issued. Create a trap manager by entering **Trap Server IP** and a community string. To define a management station as a trap manager, enter **SNMP** community strings and select the **SNMP** version.

SNMP Trap Setting **interface**

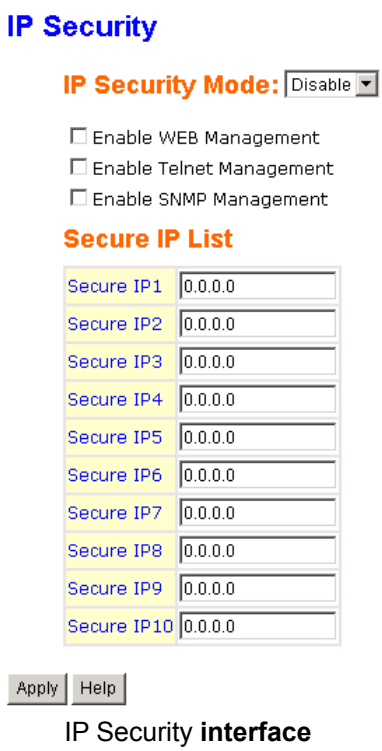
Label	Description
Server IP	Enter the server IP address to receive **Traps**
Community	Community name string for authentication purposes
Trap Version	Check **V1** or **V2**.
Add	Add trap server profile to the network
Remove	Remove trap server profile from the network
Help	Display **Help** file.

2.11 Security

Five approaches are available for enhancing the security of a switch: **IP Security, Port Security, MAC Blacklist, and MAC address Aging and 802.1x protocol.** These approaches are described below.

2.11.1 IP SECURITY

Through **IP Security** function, only IP's on the **Secure IP List** can perform switch management, provided one of the **IP Security Modes** is enabled: **Web-based, Telnet, SNMP**.



IP Security **interface**

Label	Description
IP security MODE	Enable/Disable the IP security function. When in "enable" the user can select one or more of the following three security approaches
Enable WEB Management	Check the box to enable **WEB Management**
Enable Telnet Management	Check the box to enable **Telnet Management**
Enable SNMP Management	Check the box to enable **SNMP Management**
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.
Help	Display **Help** file

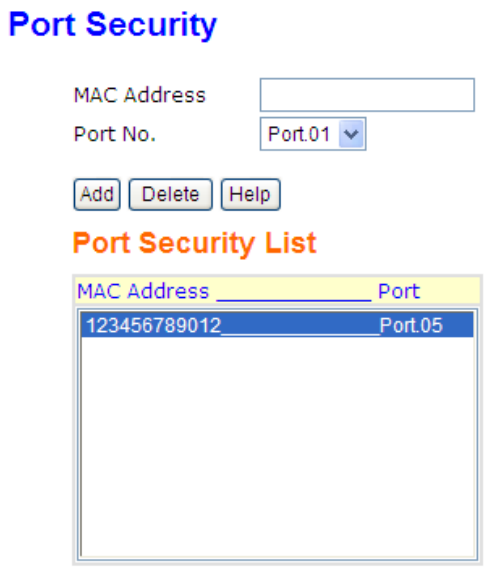
2.11.2 PORT SECURITY

Port security is a collection of "static" **MAC Addresses** (not ports on the switch) where data transmissions are deemed secure and "permitted". Transmission of data to and from addresses not on the list will be discarded.

This Example here illustrates that ONLY the host with MAC address 12:34:56:78:90:12 is allowed to access Port 5 of the switch; other hosts will not "see" the switch if plugged into Port 5.

To add a secure port, first select "Port No." on the dialogue box then type in the desired MAC address, without the connecting colons ":" (for instance, in this example, enter Mac Address "123456789012"), then click "Add" to complete the process.

To delete a secure port, select the "MAC Address-Port" from the "Port Security List" (high-lighted), then press "Delete".



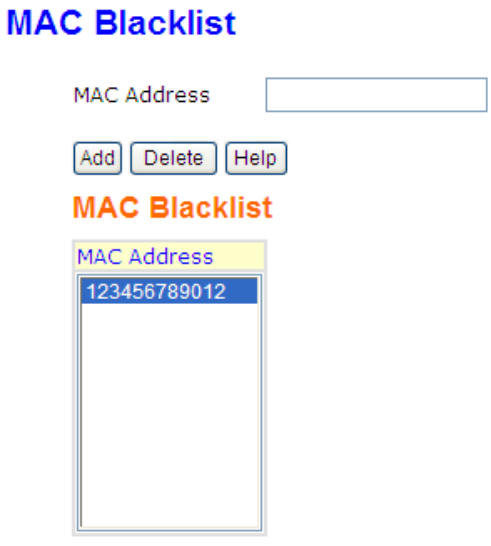
Port Security **interface**

Label	Description
MAC Address	**Manually** Input the **MAC Address** designated as a secure port.
Port No.	Select the secure port number on a switch.
Add	**Add** the MAC Address and the secure Port number to the secure ports list.
Delete	**Delete** the entry.
Help	Display **Help** file

2.11.3 MAC BLACKLIST

"Mac Blacklist" tabulates all the physical MAC addresses that are blocked from accessing the switch. This works in opposite of "Port Security" function.

To do so, first enter the MAC address to be blocked, which consists of 12 digits, then click "Add". Then the address should appear in the "Mac Address" box.



Label	Description
MAC Address	Enter **MAC Address** to the **MAC Blacklist** table.
Add	Add an **MAC Address** to the **MAC Blacklist** table.
Delete	Delete the **MAC Address** entry from the **MAC Blacklist** table.
Help	Show Display **Help** file.

2.11.4 MAC ADDRESS AGING

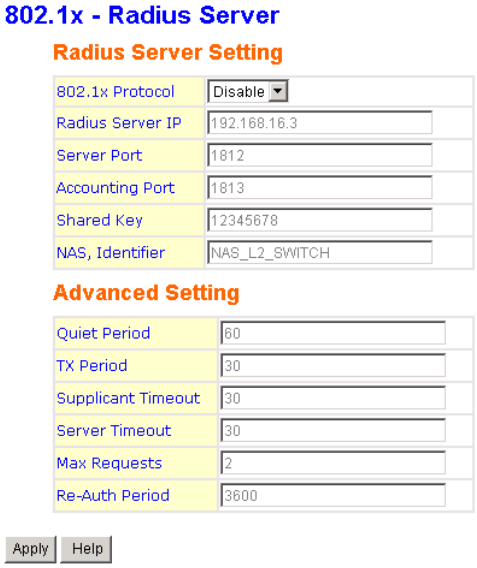
"**MAC Address Aging**", when "**Auto Flush MAC Address Table When Ports Link Down**" is checked, keeps original MAC connection (dynamic MAC Table) for a period of time. In the example, the original dynamic MAC table (connections) to the switch will remain for 300 seconds. If the "Auto Flush…" is not checked, the MAC address will disappear immediately after link down. This function speeds up the LAN connections after any momentary interruption, like a power surge or power outage.

Label	Description
MAC Address Table Aging Time: (0~3825)	Enter in seconds the default **MAC aging timer** is 300 seconds.
Auto Flush MAC Address Table When ports Link Down	Check the box to enable the function.
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.
Help	Display **Help** file.

2.12.5.1 802.1x-Radius Server Authentication

2.11.5 802.1X SERVER SETTING

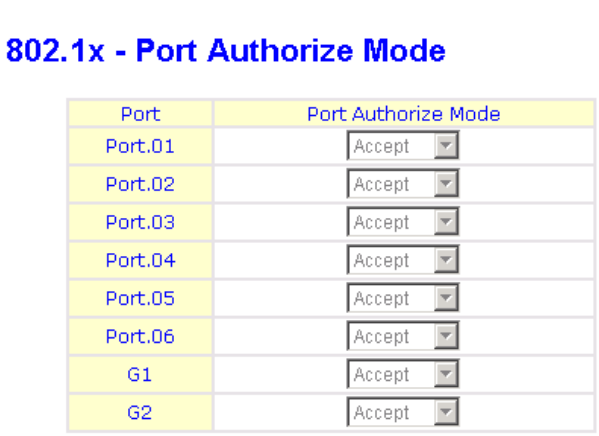
802.1x follows IEEE802 LAN infrastructures to authenticate, and subsequently to authorize the access of a device attached to a LAN port. To activate this authentication function, the user must first enable the 802.1X Radius Server.



Label	Description
802.1x Protocol	Select “Enable” to activate authentication or “disable” to otherwise. The following parameters will not appear if “**disable**” is selected.
Radius Server IP	Enter the IP address of the authentication server.
Server port	Enter the **UDP** (User Datagram Protocol) port number on the authentication server
Account port	Enter the UDP **destination port** number for accounting requests from the Radius Server.
Shared Key	Enter the “key” (30 characters max.) pre-set on the server side
NAS, Identifier	Enter the Network Access Server (NAS) ”identifier” (30 characters max.) preset on the server side
Advanced Setting	
Quiet Period	Enter the number of seconds between authentication failure and new authentication attempt
Tx Period	Enter the number of seconds between sending Extensible Authentication Protocol (**EAP**) requests.
Supplicant Timeout	Enter the number of seconds the switch must waits for a supplicant to respond to an **EAP** request.
Server Timeout	Enter the number of seconds the switch must waits for a Radius server to respond to an authentication request.
Max Requests	Enter the number of times to send packets to the supplicant.
Re-Auth Period	Enter the number of seconds for a connected client to be re-authenticated
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.
Help	Display **Help** file

2.11.5.2 Enter Port Authorization Mode

Once a Radius server is appointed the user can begin to assign each port’s authorization status: to unconditionally **accept** a port (automatic authentication), to unconditionally **reject** a port (automatic rejection for authentication), to **authorize** a port for authentication process, or simply **disable** the port from the authentication process (ignored by Radius server).

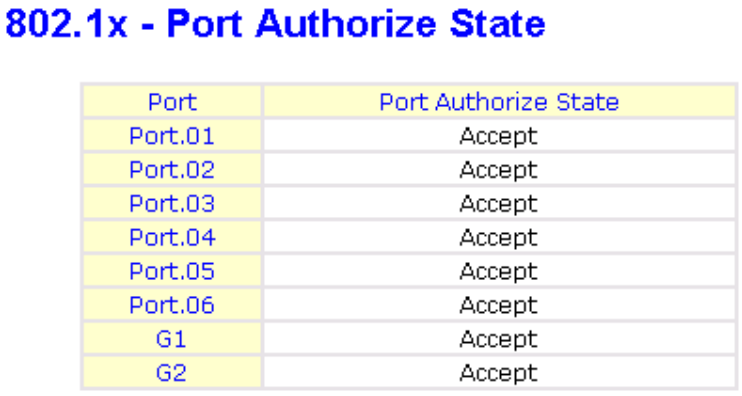


Label	Description
Port Authorization Mode	**Reject:** reject this port outright **Accept:** accept this port outright (w/o authentication needed **Authorize:** port subject to authentication (port sent to Radius) **Disable:** port not subject to authenticated (not recognized by Radius)
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.
Help	Display **Help** file.

Click **Authorization State** to view each port's status for 802.1X authentication. An example

2.11.5.3 Port Authorization Status Display

display is shown below.

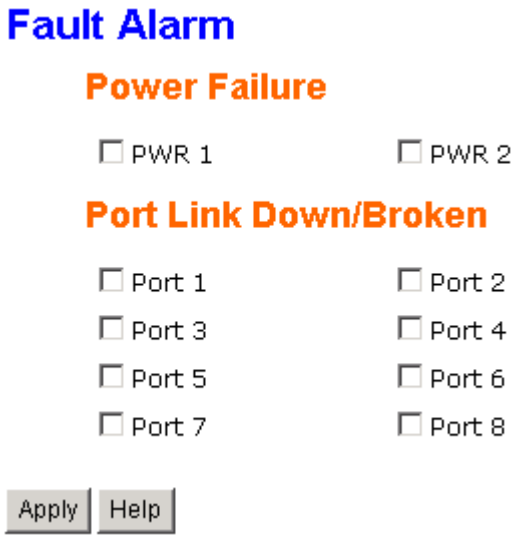


2.12 Warning (Fault Alarm Messages)

Any system fault can be delivered by physical indicators on the switch (**Fault Alarm**) or stored in **System Warning** (**SYSLOG** or **Email**). The **Fault Alarm** function controls the fault LED indicator on the switch and closes the fault relay at the bottom panel of the switch. While the fault events are stored on **SYSLOG**, and if elected, the fault messages will be sent via **E-MAIL**.

2.12.1 FAULT ALARM

When any fault event occurs, the **Fault LED** on the specific port channel switch shall come on and the relay will be closed at the same time.



Fault Alarm **interface**

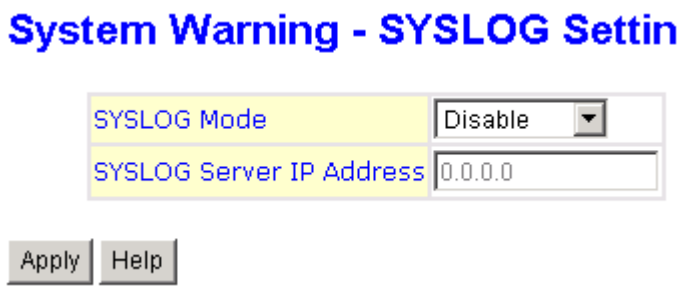
Label	Description
Power Failure	In case both boxes are checked, if **PWR 1/ PWR 2** is disconnected, a fault event is triggered. If only **PWR 1** is checked, then disconnecting PWR 2 will not trigger a fault event.
Port Link Down/Broken	Check only the port(s) which fault condition(s) will trigger a fault warning. For instance, if port 3 is not checked, the absence of connection will not cause a fault alarm.
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.
Help	**Display "Help" file.**

2.12.2 SYSTEM WARNING

System Alarm supports two warning modes: 1. **SYSLOG**. 2. **E-MAIL**. The user can monitor the fault events through one or both selected mode(s).

2.12.2.1 SYSLOG

The **SYSLOG** is a protocol for transmitting event notification messages across networks (**RFC 3164).**

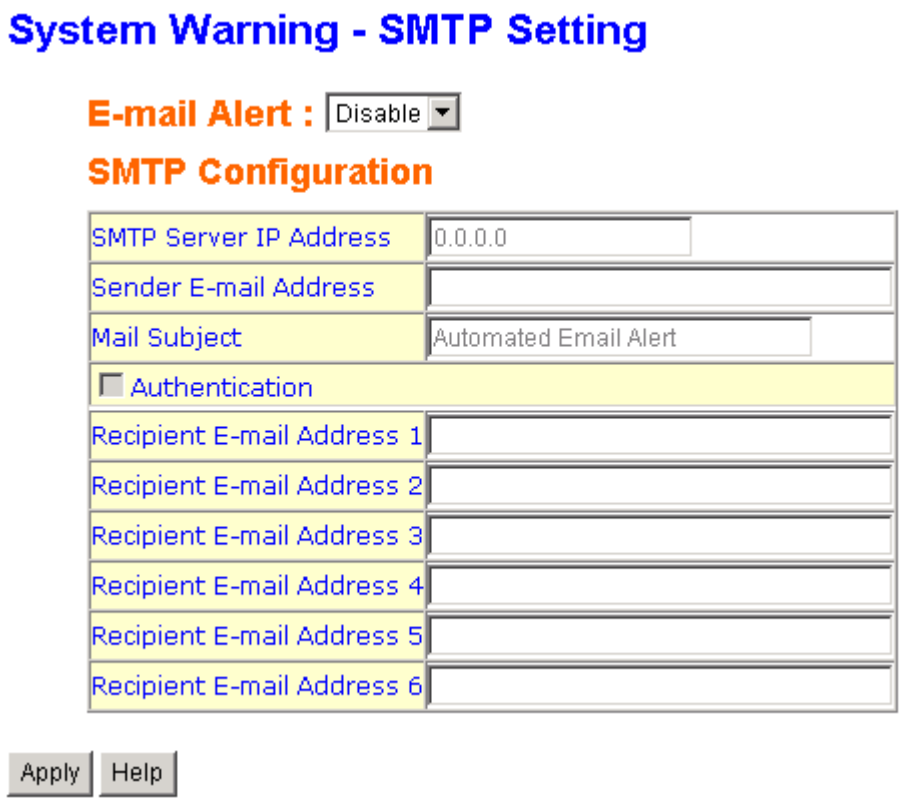


System Warning – SYSLOG Setting **interface**

Label	Description
SYSLOG Mode	**Disable**: disable **SYSLOG** **Client Only**: Store SYSLOG on the switch's memory **Server Only**: Forward SYSLOG to a remote **SYSLOG** server **Both**: Store in switch and remote server
SYSLOG Server IP Address	Enter Remote **SYSLOG Server IP address**
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.
Help	**Display "Help" file.**

2.12.2.2 SMTP (or Email Warning)

Fault events can be sent through a SMTP server in the form of Email to the authorized email addresses. **SMTP** is short for **Simple Mail Transfer Protocol** and is for e-mail transmission across the Internet (**RFC 821**).



System Warning – SMTP Setting **interface**

Label	Description
E-mail Alarm	Enable/Disable transmission system warning events by e-mail.
Sender E-mail Address	**SMTP** server IP address
Mail Subject	Subject of the mail (example: Automated Email Alert)
Authentication	If the **STMP** server requires authenticate sender, the box must be checked.
Recipient E-mail Address	The recipient's E-mail address. It supports up to 6 recipients for a message.
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.
Help	**Display "Help" file.**

2.12.2.3 Event Selection

The system allows the user to select the types of event to store or forward. Note **SYSLOG** or **SMTP** must be enabled before it is enabled.

System Warning - Event Selection

System Event

Event	SYSLOG	SMTP
System Cold Start	☐	☐
Power Status	☐	☐
SNMP Authentication Failure	☐	☐
Rapid R-Ring Topology Change	☐	☐

Port Event

Port No.	SYSLOG	SMTP
Port.01	Disable	Disable
Port.02	Disable	Disable
Port.03	Disable	Disable
Port.04	Disable	Disable
Port.05	Disable	Disable
Port.06	Disable	Disable
G1	Disable	Disable
G2	Disable	Disable

Apply Help

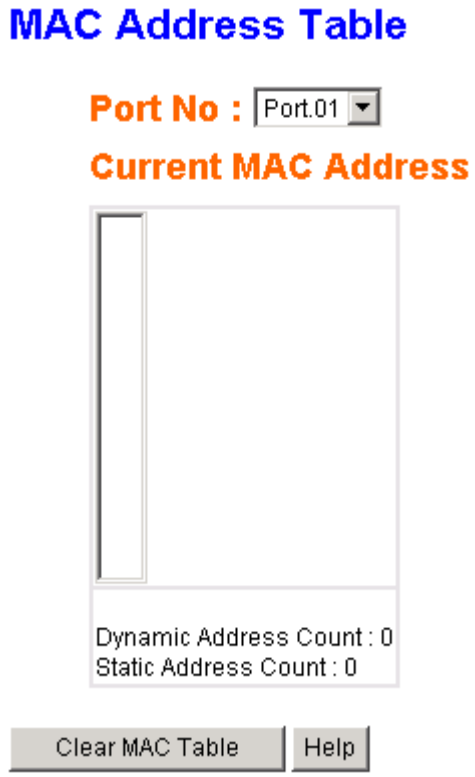
System Warning – Event Selection interface

Label	Description
System Event	
System Cold Start	Send fault alert for any system restart
Power Status	Send fault alert for power up or down (change of power state).
SNMP Authentication Failure	Send fault alert for **SNMP** authentication failure.
IA-Ring Topology Change	Send fault alert for any topology change.
Port Event	**Disable** : no triggers be sent **Link Up** : Link Up triggering a fault alert **Link Down** : Link Down triggering a fault alert **Link Up or Link Down** : Link up or Link Down triggering a fault alert
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.
Help	**Display "Help" file.**

2.13 Monitor(ing) and Diag(nosis of Individual Port)

2.13.1 MAC Address Table

In reference to IEEE 802.1 D Sections 7.9, the **MAC Address Table displays all dynamic or static MAC addresses mapped to a given port**.



MAC Address Table **interface**

Label	Description
Port NO. :	Display all (dynamic and static) MAC addresses mapped to a selected port in table.
Clear MAC Table	Clear all MAC dynamic addresses in table
Help	**Display "Help" file.**

2.13.2 Port Statistics

The Port statistics table shows the transmission statistics and link status for all ports.

Port Statistics

Port	Type	Link	State	TX Good Packet	TX Bad Packet	RX Good Packet	RX Bad Packet	TX Abort Packet	Packet Collision
Port.01	100TX	Down	Enable	0	0	0	0	0	0
Port.02	100TX	Down	Enable	0	0	0	0	0	0
Port.03	100TX	Down	Enable	0	0	0	0	0	0
Port.04	100TX	Down	Enable	0	0	0	0	0	0
Port.05	100TX	Down	Enable	0	0	0	0	0	0
Port.06	100TX	Down	Enable	0	0	0	0	0	0
G1	1000TX	Up	Enable	5358	0	10001	0	0	0
G2	1000TX	Down	Enable	0	0	0	0	0	0

Clear Help

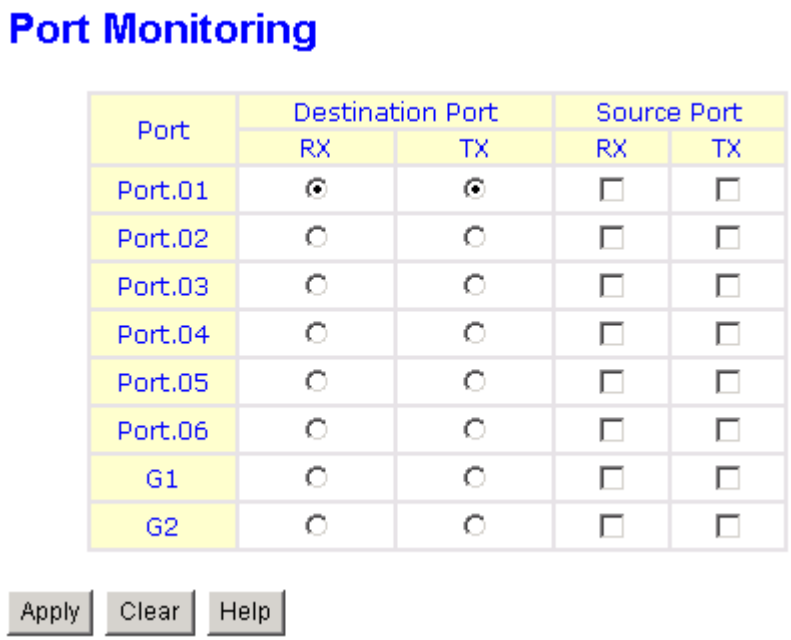
Port Statistics **interface**

Label	Description
Type	Display port transmission and media type
Link	Display port link status.
State	Display if the port is activated/deactivated (**enable/ disable**).
TX GOOD Packet	Display the number of good packets sent from this port
TX Bad Packet	Display the number of bad packets sent from this port
RX GOOD Packet	Display the number of good packets received
RX Bad Packet	Display the number of bad packets received
TX Abort Packet	Display the number of packets aborted
Packet Collision	Display the number of collisions detected
Clear	Clear all counters
Help	**Display "Help" file**

2.13.3 PORT MONITORING

A **Destination port** receives duplicated packets from one or more **Source ports**, for monitoring purposes, if theist **Rx** or **Tx** box is checked. And only one **Destination port** can be enabled at a time. Then a Rx **Destination port** can be assigned to one or more **RX** ports from the **Source Port** (s), and only one **Destination TX port** can be assigned to one or more **Source TX ports**. For instance, if **Port 01 Rx** is checked, and one wishes to direct duplicated data received by **Source port** 02 **Rx** and Port 03 **Rx** to Port **Rx** 01, then check **Source Port** 02 **Rx** and **Source Port** 03 **Rx**. Likewise, if data sent out from **Source port** 01 Tx and port 02 **Tx** is to be copied and sent to **Destination port** 03 **Tx**, then check **Destination port** 03 **Tx**, then **Source port** 02 TX and **Source port** 03 **Tx**.

If all the **Source ports** are left unchecked, then no ports are monitored.

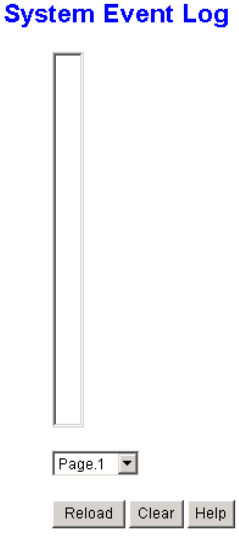


Port monitoring **interface**

Label	Description
Destination Port	A Destination Port is the port that receives a copy of frames from the source port. Check one at a time.
Source Port	Port or ports to be monitored. Check either TX/RX or both.
TX	Data transmission from the port
RX	Data received by the port.
Apply	Click **Apply** to confirm the changes; Select **File->Save** to save the setup.
Clear	Clear all entries.(disable the function)
Help	**Display "Help" file.**

2.13.4 SYSTEM EVENT LOG

If **system log client** is enabled, **system Event Log** will appear as follows.



2.14 Front Panel

Display the EH front panel by clicking **Front Panel**. Click Close to close **Front Panel**.

2.15 Save Configuration

Use **Save Configuration** to save current configuration to the flash memory to avoid data loss during power off or system reset.

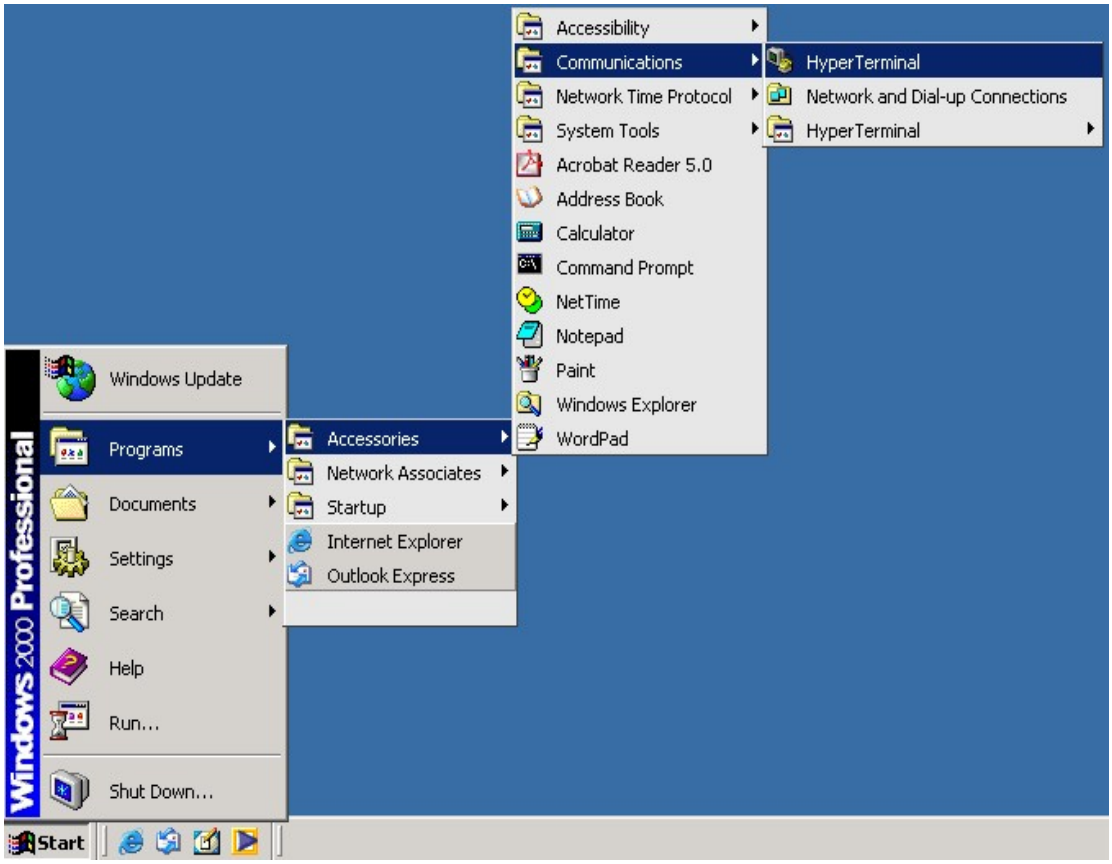
Part 3 Configuration via Command Line Interface (CLI)

The EH Series supports Configuration by the Command Line Interface or CLI. The user may manage the switch via its console port or via Telnet.

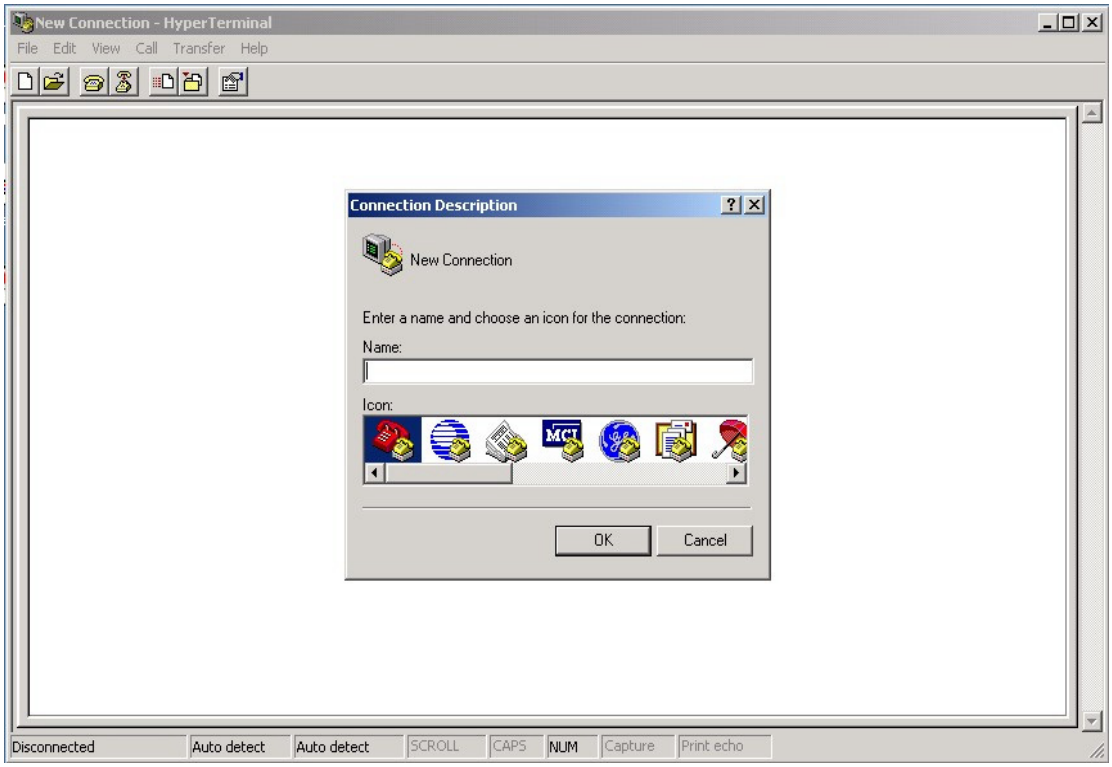
3.1 CLI Management via a PC's Serial-console Port

Before Configuring a switch via its serial console port, use an RJ45-to-DB9-F cable to connect the EH Switch's **Console** port (RJ-45 connector) to the PC's **COM** port (serial port number must be defined by the user) of choice. Then follow the steps below.

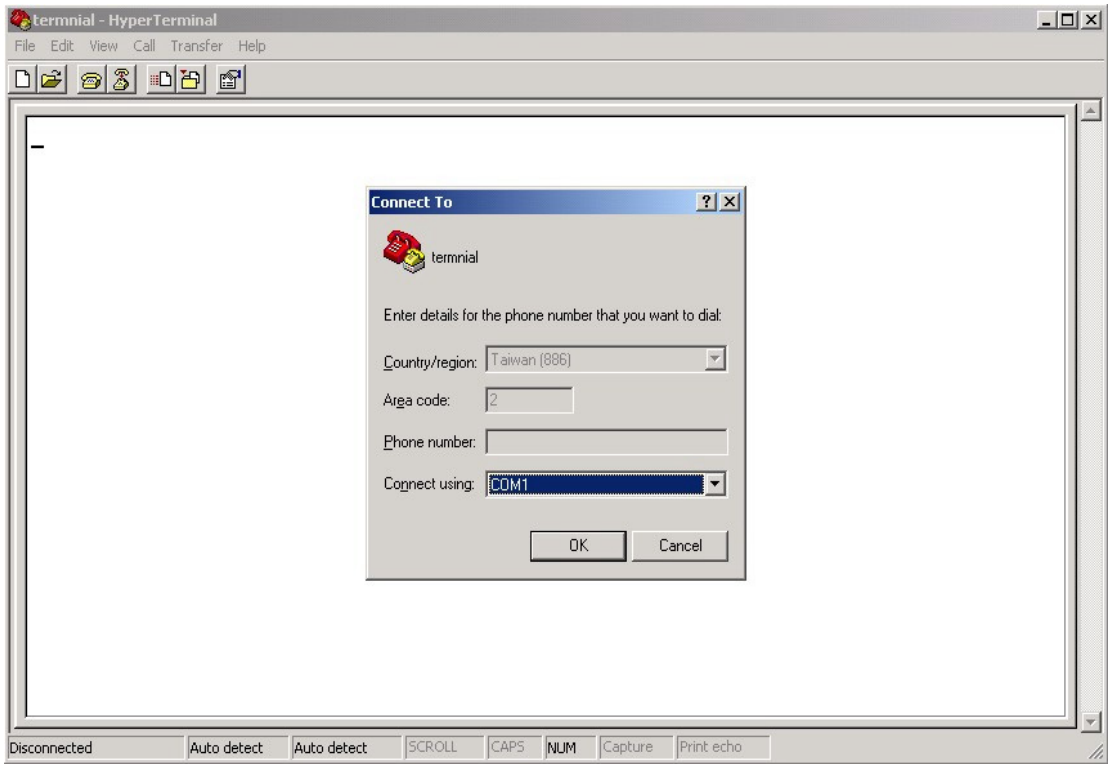
(1) On **Windows desktop**, click **Start -> All Programs -> Accessories -> Communications -> Hyper Terminal**



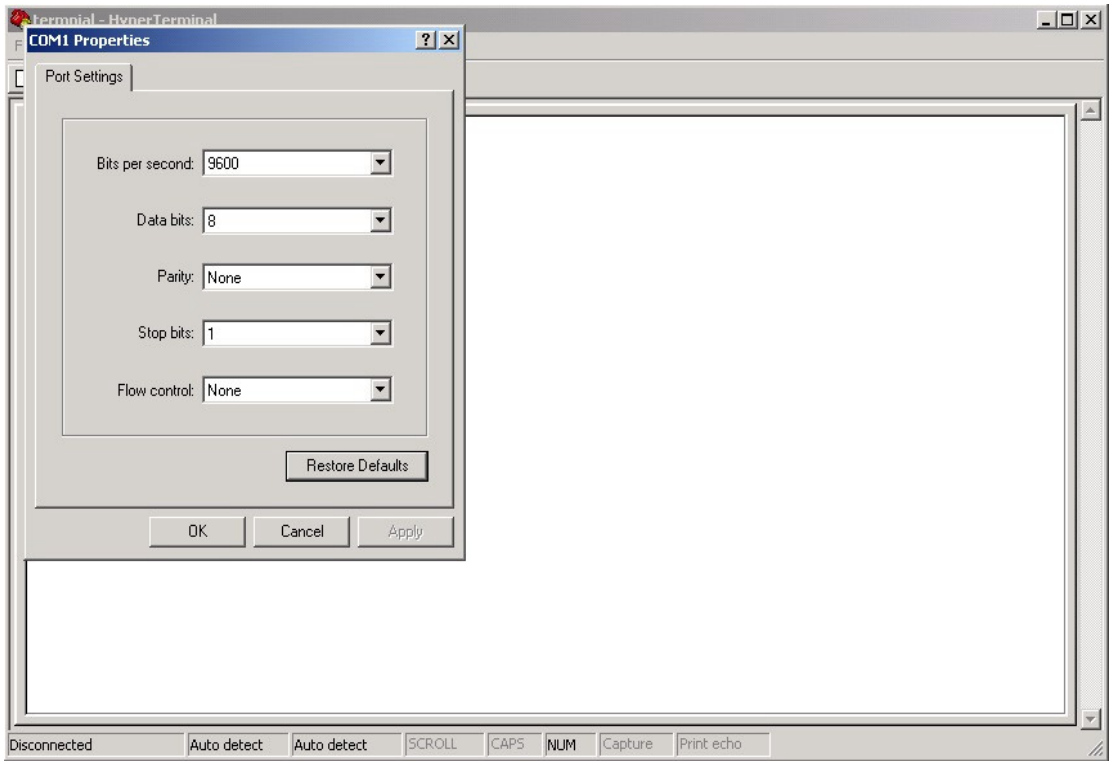
(2) Input a name for the new connection (Example: Myconnection)



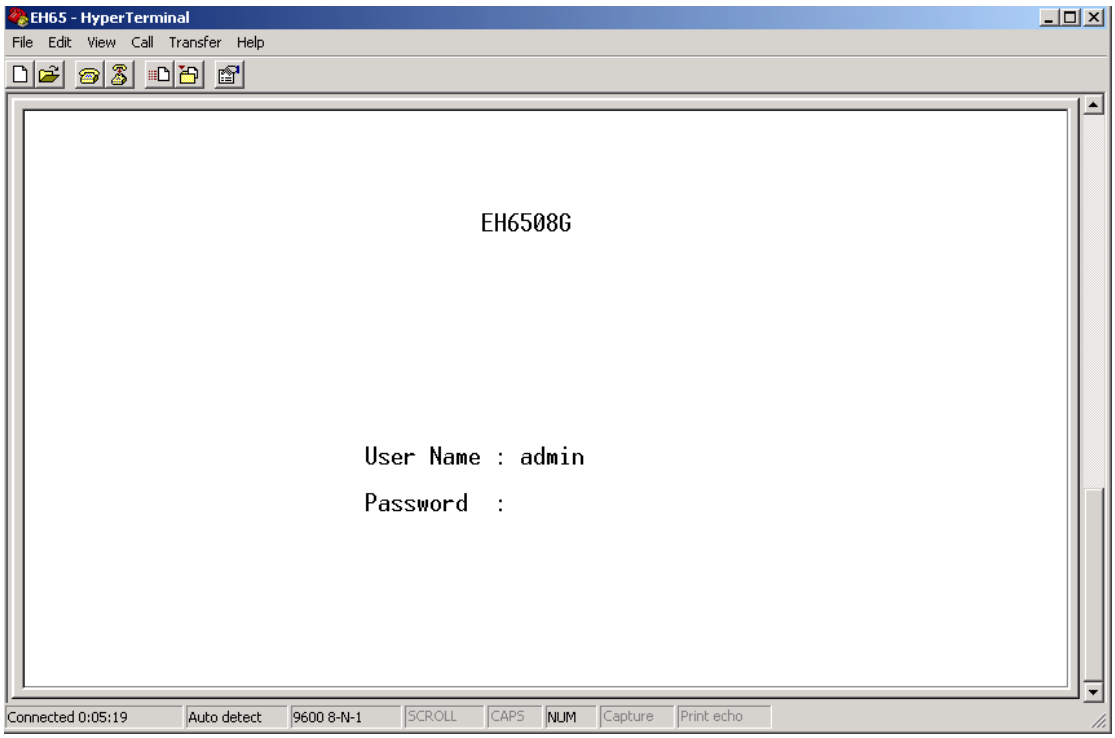
(3) On "**Connect using**", select a **COM** port from **Com1, Com2 (default), Com3 or Com4**



(4) The COM port properties setting: “9600” **Bits per second**, “8” **Data bits**, “None” **Parity**, “1” **Stop bit** and “none” **Flow control**.



(5) The Console login screen shall appear. Enter **User Name (default: admin)** and **Password** (default: blank) then press **Enter**.



3.2 CLI Management via Telnet

The user can use **Telnet** to configure a EH switch.

Note that the default values are:

IP Address: **10.0.50.100**

Subnet Mask: **255.255.0.0**

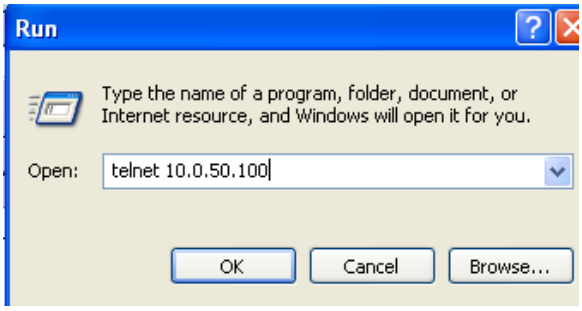
Default Gateway: **10.0.0.254**

User Name: **admin**

Password: “NULL” Leave it blank)

Follow the steps below to access the console via Telnet.

(1) Telnet to the EH Switch’s IP address using the Windows’ **Start->Run** command (or from the MS-DOS prompt).



(2) The login screen shall appear. Enter **User Name** and **Password** then press **Enter,** then “**the switch >**” prompt shall appear (while in User **EXEC** mode)

3.3 CLI List of Commands

3.3.1 Command Level: Prompt and Exit Commands in Various Modes

While in **Mode** below	Access Command	Prompt	Exit Command	Model Access
User EXEC	Begin a new session (after pressing **enter** on "**password"**)	**switch>**	**logout** or **quit**.	• Enter **menu** mode • Display system information.
Privileged EXEC	Enter **enable** while in **user EXEC** mode to change to **Privileged EXEC** mode	**switch#**	**disable**	• Display advance function status • Save configuration
Global configuration	Enter **configure** while in **Privileged EXEC** mode.	**switch(config)#**	**exit** or **end**	Configure global switch parameters
VLAN database	Enter **vlan database** while in **Privileged EXEC** mode.	**switch(vlan)#**	**exit**	Configure **VLAN**-specific parameters
Interface configuration	Enter **interface command (with a specific interface)** while in **Global configuration** mode	**switch(config-if)#**	**exit** or **end**	Configure switch interface parameters

3.3.2 List of Modes and their Symbols at Command Level

Mode	Command Mode Symbol
User EXEC	**E**
Privileged EXEC	**P**
Global configuration	**G**
VLAN database	**V**
Interface configuration	**I**

3.3.3 List of System Commands

System Command	Mode	Description	Example
show config	E	Display switch configuration	switch>show config
show terminal	P	Display console information	switch#show terminal
menu	E	Enter menu mode	switch>menu
write memory	P	Save user configuration into permanent flash memory	switch#write memory
system name [System Name]	G	Enter system name	switch(config)#system name xxx

system location [System Location]	G	Enter switch system location string	switch(config)#system location xxx
system description [System Description]	G	Enter switch system description string	switch(config)#system description xxx
system contact [System Contact]	G	Enter switch system contact window string	switch(config)#system contact xxx
show system-info	E	Display system information	switch>show system-info
ip address [Ip-address] [Subnet-mask] [Gateway]	G	Configure switch IP address	switch(config)#ip address 10.0.50.52 255.255.255.0 10.0.50.54
ip dhcp	G	Enable DHCP Client function	switch(config)#ip dhcp
show ip	P	Display switch IP	switch#show ip
no ip dhcp	G	Disable DHCP Client function	switch(config)#no ip dhcp
reload	G	Halt and perform a cold restart	switch(config)#reload
default	G	Restore to default values	Switch(config)#default
admin username [Username]	G	Change login username (maximum 10 words)	switch(config)#admin username xxxxxx
admin password [Password]	G	Change login password (maximum 10 words)	switch(config)#admin password xxxxxx
show admin	P	Display administrator information	switch#show admin
dhcpserver enable	G	Enable DHCP Server	switch(config)#dhcpserver enable
dhcpserver lowip [Low IP]	G	Configure low IP address for IP pool	switch(config)# dhcpserver lowip 10.0.50.54
dhcpserver highip [High IP]	G	Configure high IP address for IP pool	switch(config)# dhcpserver highip 10.0.50.50
dhcpserver subnetmask [Subnet mask]	G	Configure subnet mask for DHCP Client	switch(config)#dhcpserver subnetmask 255.255.255.0
dhcpserver gateway [Gateway]	G	Configure gateway for DHCP Client	switch(config)#dhcpserver gateway 10.0.50.56
dhcpserver dnsip [DNS IP]	G	Configure DNS IP for DHCP Client	switch(config)# dhcpserver dnsip 10.0.50.54
dhcpserver leasetime [Hours]	G	Configure lease time (in hours)	switch(config)#dhcpserver leasetime 1
dhcpserver ipbinding [IP address]	I	Enter static IP for DHCP Client by port	switch(config)#interface fastEthernet 2 switch(config-if)#dhcpserver ipbinding 10.0.50.54
show dhcpserver configuration	P	Display configuration of DHCP server	switch#show dhcpserver configuration
show dhcpserver clients	P	Display client entries of DHCP server	switch#show dhcpserver clinets
show dhcpserver ip-binding	P	Display IP-Binding information of the DHCP server	switch#show dhcpserver ip-binding
no dhcpserver	G	Disable DHCP server function	switch(config)#no dhcpserver
security enable	G	Activate IP security function	switch(config)#security enable

security http	G	Activate HTTP server security (only the secure IP can access the server)	switch(config)#security http
security telnet	G	Activate telnet security	switch(config)#security telnet
security ip [Index(1..10)] [IP Address]	G	Enter secure port(s) IP	switch(config)#security ip 1 10.0.50.55
show security	P	Display switch security information	switch#show security
no security	G	Disable IP security function	switch(config)#no security
no security http	G	Disable IP security for HTTP server access	switch(config)#no security http
no security telnet	G	Disable IP security for telnet access	switch(config)#no security telnet

3.3.4 List of Port Commands

Port Command	Mode	Description	Example
interface fastEthernet [Portid]	G	Define port ID	switch(config)#interface fastEthernet 2
duplex [full | half]	I	Specify either full duplex or half duplex transmission for Ethernet Ports	switch(config)#interface fastEthernet 2 switch(config-if)#duplex full
speed [10|100|1000|auto]	I	Specify speed for Fast Ethernet ports (only a giga port can accept “1000”)	switch(config)#interface fastEthernet 2 switch(config-if)#speed 100
flowcontrol mode [Symmetric|Asymmetric]	I	Select between “symmetric” or “asymmetric” traffic pattern	switch(config)#interface fastEthernet 2 switch(config-if)#flowcontrol mode Asymmetric
no flowcontrol	I	Disable flow control of interface	switch(config-if)#no flowcontrol
security enable	I	Enable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#security enable
no security	I	Disable security of interface	switch(config)#interface fastEthernet 2 switch(config-if)#no security
bandwidth type all	I	Enter interface ingress limit frame type to accept “all” frames	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type all
bandwidth type broadcast-multicast-flooded-unicast	I	Ingress to accept “broadcast, multicast, and flooded unicast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast-flooded-unicast
bandwidth type broadcast-multicast	I	Ingress to accept “broadcast and multicast frame”	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-multicast

bandwidth type broadcast-only	I	Ingress to “only accept “broadcast frames only	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth type broadcast-only
bandwidth in [Value]	I	Input bandwidth: from 100 kbps to 102400 kbps for a Fast Ethernet port, or up to 256000 kbps for a giga port; “0” or zero means “no limit”.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth in 100
bandwidth out [Value]		Output bandwidth: 100 kbps to 102400 kbps for a Fast Ethernet port or up to 256000 kbps for a giga port, And “0” or zero means no limit.	switch(config)#interface fastEthernet 2 switch(config-if)#bandwidth out 100
show bandwidth	I	Display interfaces bandwidth control	switch(config)#interface fastEthernet 2 switch(config-if)#show bandwidth
state [Enable | Disable]	I	Force an Ethernet port to “Enable” or “Disable” state	switch(config)#interface fastEthernet 2 switch(config-if)#state Disable
show interface configuration	I	show interface configuration status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface configuration
show interface status	I	show interface status	switch(config)#interface fastEthernet 2 switch(config-if)#show interface status
show interface accounting	I	show interface counter	switch(config)#interface fastEthernet 2 switch(config-if)#show interface accounting
no accounting	I	Clear interface accounting information	switch(config)#interface fastEthernet 2 switch(config-if)#no accounting

3.3.5 LIST OF TRUNK COMMANDS

Trunk Command	Mode	Description	Example
aggregator priority [1~65535]	G	Enter port group system priority	switch(config)#aggregator priority 22
aggregator activityport [Port Numbers]	G	Enter activity port	switch(config)#aggregator activityport 2
aggregator group [GroupID] [Port-list] lacp workp [Workport]	G	Assign a trunk group with LACP active. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6) [Workport]: The amount of work ports, this value could not be less than zero or be large than the amount of member ports.	switch(config)#aggregator group 1 1-4 lacp workp 2 or switch(config)#aggregator group 2 1,4,3 lacp workp 3

aggregator group [GroupID] [Port-list] nolacp	G	Assign a static trunk group. [GroupID] :1~3 [Port-list]:Member port list, This parameter could be a port range(ex.1-4) or a port list separate by a comma(ex.2, 3, 6)	switch(config)#aggregator group 1 2-4 nolacp or switch(config)#aggreator group 1 3,1,2 nolacp
show aggregator	P	Display the information of trunk group	switch#show aggregator
no aggregator lacp [GroupID]	G	Disable the LACP function of trunk group	switch(config)#no aggreator lacp 1
no aggregator group [GroupID]	G	Remove a trunk group	switch(config)#no aggreator group 2

3.3.6 LIST OF VLAN COMMANDS

VLAN Command	Mode	Description	Example
vlan database	P	Enter VLAN configure mode	switch#vlan database
vlan [8021q | gvrp]	V	To set switch **VLAN** mode.	switch(vlan)# vlanmode 8021q or switch(vlan)# vlanmode gvrp
no vlan [VID]	V	Disable vlan group(by VID)	switch(vlan)#no vlan 2
no gvrp	V	Disable GVRP	switch(vlan)#no gvrp
IEEE 802.1Q VLAN			
vlan 8021q port [PortNumber] access-link untag [UntaggedVID]	V	Assign a access link for **VLAN** by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 access-link untag 33
vlan 8021q port [PortNumber] trunk-link tag [TaggedVID List]	V	Assign a trunk link for **VLAN** by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)#vlan 8021q port 3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q port 3 trunk-link tag 3-20
vlan 8021q port [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for **VLAN** by port, if the port belong to a trunk group, this command can't be applied.	switch(vlan)# vlan 8021q port 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q port 3 hybrid-link untag 5 tag 6-8
vlan 8021q aggreator [TrunkID] access-link untag [UntaggedVID]	V	Assign a access link for **VLAN** by trunk group	switch(vlan)#vlan 8021q aggreator 3 access-link untag 33
vlan 8021q	V	Assign a trunk link for **VLAN**	switch(vlan)#vlan 8021q aggreator

aggreator [TrunkID] trunk-link tag [TaggedVID List]		by trunk group	3 trunk-link tag 2,3,6,99 or switch(vlan)#vlan 8021q aggreator 3 trunk-link tag 3-20
vlan 8021q aggreator [PortNumber] hybrid-link untag [UntaggedVID] tag [TaggedVID List]	V	Assign a hybrid link for **VLAN** by trunk group	switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 4 tag 3,6,8 or switch(vlan)# vlan 8021q aggreator 3 hybrid-link untag 5 tag 6-8
show vlan [VID] or show vlan	V	Display **VLAN** information	switch(vlan)#show vlan 23

3.3.7 LIST OF SPANNING TREE COMMANDS

Spanning Tree Command	Mode	Description	Example
spanning-tree enable	G	Enable spanning tree	switch(config)#spanning-tree enable
spanning-tree priority [0~61440]	G	Configure spanning tree priority parameter	switch(config)#spanning-tree priority 32767
spanning-tree max-age [seconds]	G	Use the spanning-tree max-age global configuration command to change the interval between messages the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputed the Spanning Tree Protocol (STP) topology.	switch(config)# spanning-tree max-age 15
spanning-tree hello-time [seconds]	G	Use the spanning-tree hello-time global configuration command to specify the interval between hello bridge protocol data units (BPDUs).	switch(config)#spanning-tree hello-time 3
spanning-tree forward-time [seconds]	G	Use the spanning-tree forward-time global configuration command to set the forwarding-time for the specified spanning-tree instances. The forwarding time determines how long each of the listening and learning states last before the port begins forwarding.	switch(config)# spanning-tree forward-time 20
stp-path-cost	I	Use the spanning-tree cost	switch(config)#interface

[1~200000000]		interface configuration command to set the path cost for Spanning Tree Protocol (STP) calculations. In the event of a loop, spanning tree considers the path cost when selecting an interface to place into the forwarding state.	fastEthernet 2 switch(config-if)#stp-path-cost 20
stp-path-priority [Port Priority]	I	Use the spanning-tree port-priority interface configuration command to configure a port priority that is used when two switches tie for position as the root switch.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-path-priority 127
stp-admin-p2p [Auto|True|False]	I	Admin P2P of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-p2p Auto
stp-admin-edge [True|False]	I	Admin Edge of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-edge True
stp-admin-non-stp [True|False]	I	Admin NonSTP of STP priority on this interface.	switch(config)#interface fastEthernet 2 switch(config-if)# stp-admin-non-stp False
Display spanning-tree	E	Display a summary of the spanning-tree states.	switch>show spanning-tree

3.3.8 LIST OF QOS COMMANDS

QoS Command	Mode	Description	Example
qos policy [weighted-fair|strict]	G	Select QOS policy scheduling	switch(config)#qos policy weighted-fair
qos prioritytype [port-based|cos-only|tos-only|cos-first|tos-first]	G	Setting of QOS priority type	switch(config)#qos prioritytype
qos priority portbased [Port] [lowest|low|middle|high]	G	Configure Port-based Priority	switch(config)#qos priority portbased 1 low
qos priority cos [Priority][lowest|low|middle|high]	G	Configure COS Priority	switch(config)#qos priority cos 22 middle
qos priority tos [Priority][lowest|low|middle|high]	G	Configure TOS Priority	switch(config)#qos priority tos 3 high
show qos	P	Display the information of QoS configuration	switch>show qos
no qos	G	Disable QoS function	switch(config)#no qos

3.3.9 LIST OF IGMP COMMANDS

IGMP Command	Mode	Description	Example
igmp enable	G	Enable IGMP snooping function	switch(config)#igmp enable

Igmp-query auto	G	Enter IGMP query to auto mode	switch(config)#Igmp-query auto
Igmp-query force	G	Enter IGMP query to force mode	switch(config)#Igmp-query force
show igmp configuration	P	Displays the details of an IGMP configuration.	switch#show igmp configuration
show igmp multi	P	Displays the details of an IGMP snooping entries.	switch#show igmp multi
no igmp	G	Disable IGMP snooping function	switch(config)#no igmp
no igmp-query	G	Disable IGMP query	switch#no igmp-query

3.3.10 List of MAC/Filter Table commands

MAC/Filter Table Command	Mode	Description	Example
mac-address-table static hwaddr [MAC]	I	Configure MAC address table of interface (static).	switch(config)#interface fastEthernet 2 switch(config-if)#mac-address-table static hwaddr 000012345678
mac-address-table filter hwaddr [MAC]	G	Configure MAC address table(filter)	switch(config)#mac-address-table filter hwaddr 000012348678
show mac-address-table	P	Display all MAC address table	switch#show mac-address-table
show mac-address-table static	P	Display static MAC address table	switch#show mac-address-table static
show mac-address-table filter	P	Display filter MAC address table.	switch#show mac-address-table filter
no mac-address-table static hwaddr [MAC]	I	Remove an entry of MAC address table of interface (static)	switch(config)#interface fastEthernet 2 switch(config-if)#no mac-address-table static hwaddr 000012345678
no mac-address-table filter hwaddr [MAC]	G	Remove an entry of MAC address table (filter)	switch(config)#no mac-address-table filter hwaddr 000012348678
no mac-address-table	G	Remove dynamic entry of MAC address table	switch(config)#no mac-address-table

3.3.11 List of SNMP Commands

SNMP Command	Mode	Description	Example
SNMP agent-mode [v1v2c | v3]	G	Select the agent mode of **SNMP**	switch(config)#snmp agent-mode v1v2c
SNMP-server host [IP address] community [Community-string] trap-version [v1|v2c]	G	Configure **SNMP** server host information and community string	switch(config)#snmp-server host 10.0.50.54 community public trap-version v1 (remove) Switch(config)# no snmp-server host 10.0.50.54
SNMP community-	G	Configure the community string right	switch(config)#snmp community-strings public right RO

strings [Community-string] right [RO|RW]			or switch(config)#snmp community-strings public right RW
SNMP snmpv3-user [User Name] password [Authentication Password] [Privacy Password]	G	Configure the userprofile for **SNMP**V3 agent. Privacy password could be empty.	switch(config)#snmp snmpv3-user test01 password AuthPW PrivPW
show **SNMP**	P	Display SNMP configuration	switch#show snmp
show **SNMP**-server	P	Display specified trap server information	switch#show snmp-server
no **SNMP** community-strings [Community]	G	Remove the specified community.	switch(config)#no snmp community-strings public
no **SNMP** snmpv3-user [User Name] password [Authentication Password] [Privacy Password]	G	Remove specified user of SNMPv3 agent. Privacy password could be empty.	switch(config)# no snmp snmpv3-user test01 password AuthPW PrivPW
no **SNMP**-server host [Host-address]	G	Remove the SNMP server host.	switch(config)#no snmp-server 10.0.50.54

3.3.12 LIST OF PORT MIRRORING COMMANDS

Port Mirroring Command	Mode	Description	Example
monitor rx	G	Enter RX destination port of monitor function	switch(config)#monitor rx
monitor tx	G	Enter TX destination port of monitor function	switch(config)#monitor tx
show monitor	P	Display port monitor information	switch#show monitor
monitor [RX|TX|Both]	I	Configure source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#monitor RX
show monitor	I	Display port monitor information	switch(config)#interface fastEthernet 2 switch(config-if)#show monitor
no monitor	I	Disable source port of monitor function	switch(config)#interface fastEthernet 2 switch(config-if)#no monitor

3.3.13 LIST OF 802.1X COMMANDS

802.1x command Commands	Mode	Description	Example
8021x enable	G	Use the 802.1x global configuration command to enable 802.1x protocols.	switch(config)# 8021x enable
8021x system radiousip [IP address]	G	Use the 802.1x system radious IP global configuration command to change the radious server IP.	switch(config)# 8021x system radiousip 10.0.50.54
8021x system serverport [port ID]	G	Use the 802.1x system server port global configuration command to change the radious server port	switch(config)# 8021x system serverport 1815
8021x system accountport [port ID]	G	Use the 802.1x system account port global configuration command to change the accounting port	switch(config)# 8021x system accountport 1816
8021x system sharekey [ID]	G	Use the 802.1x system share key global configuration command to change the shared key value.	switch(config)# 8021x system sharekey 123456
8021x system nasid [words]	G	Use the 802.1x system nasid global configuration command to change the NAS ID	switch(config)# 8021x system nasid test1
8021x misc quietperiod [sec.]	G	Use the 802.1x misc quiet period global configuration command to specify the quiet period value of the switch.	switch(config)# 8021x misc quietperiod 10
8021x misc txperiod [sec.]	G	Use the 802.1x misc TX period global configuration command to set the TX period.	switch(config)# 8021x misc txperiod 5
8021x misc supportimeout [sec.]	G	Use the 802.1x misc supp timeout global configuration command to set the supplicant timeout.	switch(config)# 8021x misc supportimeout 20
8021x misc servertimeout [sec.]	G	Use the 802.1x misc server timeout global configuration command to set the server timeout.	switch(config)#8021x misc servertimeout 20
8021x misc maxrequest [number]	G	Use the 802.1x misc max request global configuration command to set the MAX requests.	switch(config)# 8021x misc maxrequest 3
8021x misc reauthperiod [sec.]	G	Use the 802.1x misc reauth period global configuration command to set the reauth period.	switch(config)# 8021x misc reauthperiod 3000
8021x	I	Use the 802.1x port state interface	switch(config)#interface fastethernet

portstate [disable | reject | accept | authorize]		configuration command to set the state of the selected port.	3 switch(config-if)#8021x portstate accept
show 8021x	E	Display a summary of the 802.1x properties and also the port sates.	switch>show 8021x
no 8021x	G	Disable 802.1x function	switch(config)#no 8021x

3.3.14 List of TFTP Commands

TFTP Command	Mode	Description	Defaults Example
backup flash:backup_cfg	G	Save configuration to TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#backup flash:backup_cfg
restore flash:restore_cfg	G	Get configuration from TFTP server and need to specify the IP of TFTP server and the file name of image.	switch(config)#restore flash:restore_cfg
upgrade flash:upgrade_fw	G	Upgrade firmware by TFTP and need to specify the IP of TFTP server and the file name of image.	switch(config)#upgrade lash:upgrade_fw

3.3.15 List of SYSLOG, SMTP, EVENT Commands

SYSLOG, SMTP, EVENT Command	Mode	Description	Example
systemlog ip [IP address]	G	Enter System log server IP address.	switch(config)# systemlog ip 10.0.50.58
systemlog mode [client|server|both]	G	Specified the log mode	switch(config)# systemlog mode both
show systemlog	E	Display system log	Switch>show systemlog
show systemlog	P	Display system log's client & server information	switch#show systemlog
no systemlog	G	Disable systemlog functon	switch(config)#no systemlog
smtp enable	G	Enable SMTP function	switch(config)#smtp enable
smtp serverip [IP address]	G	Configure SMTP server IP	switch(config)#smtp serverip 10.0.50.59
smtp authentication	G	Enable SMTP authentication	switch(config)#smtp authentication
smtp account [account]	G	Configure authentication account	switch(config)#smtp account User
smtp password [password]	G	Configure authentication password	switch(config)#smtp password
smtp rcptemail [Index] [Email address]	G	Define e-mail (for reception) Address	switch(config)#smtp rcptemail 1 Alert@test.com
show smtp	P	Display SMTP information	switch#show smtp
no smtp	G	Disable SMTP function	switch(config)#no smtp
event device-cold-start [Systemlog|SMTP|Both]	G	Enter cold start event	switch(config)#event device-cold-start both
event authentication-failure	G	Enter Authentication failure event	switch(config)#event authentication-failure both

[Systemlog|SMTP|Both]			
event iA-ring-topology-change [Systemlog|SMTP|Both]	G	Enter iA-ring “topology change” event	switch(config)#event iA-Ring-topology-change both
event systemlog [Link-UP|Link-Down|Both]	I	Enter system event	switch(config)#interface fastethernet 3 switch(config-if)#event systemlog both
event smtp [Link-UP|Link-Down|Both]	I	Enter SMTP event	switch(config)#interface fastethernet 3 switch(config-if)#event smtp both
show event	P	Display event selection	switch#show event
no event device-cold-start	G	Disable cold start event	switch(config)#no event device-cold-start
no event authentication-failure	G	Disable Authentication failure event	switch(config)#no event authentication-failure
no event iA-Ring-topology-change	G	Disable iA ring topology change event	switch(config)#no event iA-Ring-topology-change
no event systemlog	I	Disable system event	switch(config)#interface fastethernet 3 switch(config-if)#no event systemlog
no event smpt	I	Disable SMTP event	switch(config)#interface fastethernet 3 switch(config-if)#no event smtp
show systemlog	P	Display system log’s client & server information	switch#show systemlog

3.3.16 List of SNTP Commands

SNTP Command	Mode	Description	Example
sntp enable	G	Enable SNTP function (If SNTP is disable, skip the following commands)	switch(config)#sntp enable
sntp daylight	G	Enable daylight saving time (only if SNTP function is in “enable”)	switch(config)#sntp daylight
sntp daylight-period [Start time] [End time]	G	Enter period of daylight saving time [yyyymmdd-hh:mm]	switch(config)# sntp daylight-period 20060101-01:01 20060202-01-01
sntp daylight-offset [Minute]	G	Enter offset of daylight saving time in minutes	switch(config)#sntp daylight-offset 3
sntp ip [IP]	G	Enter SNTP server IP 137.189.6.18 is Hong Kong SNTP	switch(config)#sntp ip 137.189.6.18
sntp timezone [Timezone]	G	Enter timezone index which can be found with “show sntp timzezone” command	switch(config)#sntp timezone 22
show sntp	P	Display SNTP information	switch#show sntp
show sntp timezone	P	Display index number in time zone list; I for Eniwetok, Kwajalein; 5 for US Pacific time; 22 for Casablanca, Monrovia	switch#show sntp timezone
no sntp	G	Disable SNTP function	switch(config)#no sntp

no sntp daylight	G	Disable daylight saving time	switch(config)#no sntp daylight

3.3.17 LIST OF IA-RING COMMANDS

IA-Ring Command	Mode	Description	Example
iA-Ring enable	G	Enable iA-Ring	switch(config)#iA-Ring enable
iA-Ring master	G	Enable iA ring master	switch(config)# iA-Ring master
iA-Ring couplering	G	Enable coupling ring	switch(config)# iA-Ring couplering
iA-Ring dualhoming	G	Enable dual homing ring	switch(config)# iA-Ring dualhoming
iA-Ring ringport [1st Ring Port] [2nd Ring Port]	G	Configure Primary and back Ring Master Ports; In the example at the right, port 7 is the primary ring master while port 8 is the backup	switch(config)# iA-Ring ringport 7 8
iA-Ring couplingport [Coupling Port]	G	Assign Coupling Port number	switch(config)# iA-Ring couplingport 1
iA-Ring controlport [Control Port]	G	Assign Control Port	switch(config)# iA-Ring controlport 2
iA-Ring homingport [Dual Homing Port]	G	Assign Dual Homing Port number	switch(config)# iA-Ring homingport 3
show iA-Ring	P	Display iA Ring information	switch#show iA-Ring
no iA-Ring	G	Disable iA-Ring	switch(config)#no iA-Ring
no iA-Ring master	G	Disable ring master	switch(config)# no iA-Ring master
no iA-Ring couplering	G	Disable couple ring	switch(config)# no iA-Ring couplering
no iA-Ring dualhoming	G	Disable dual homing ring	switch(config)# no iA-Ring dualhoming

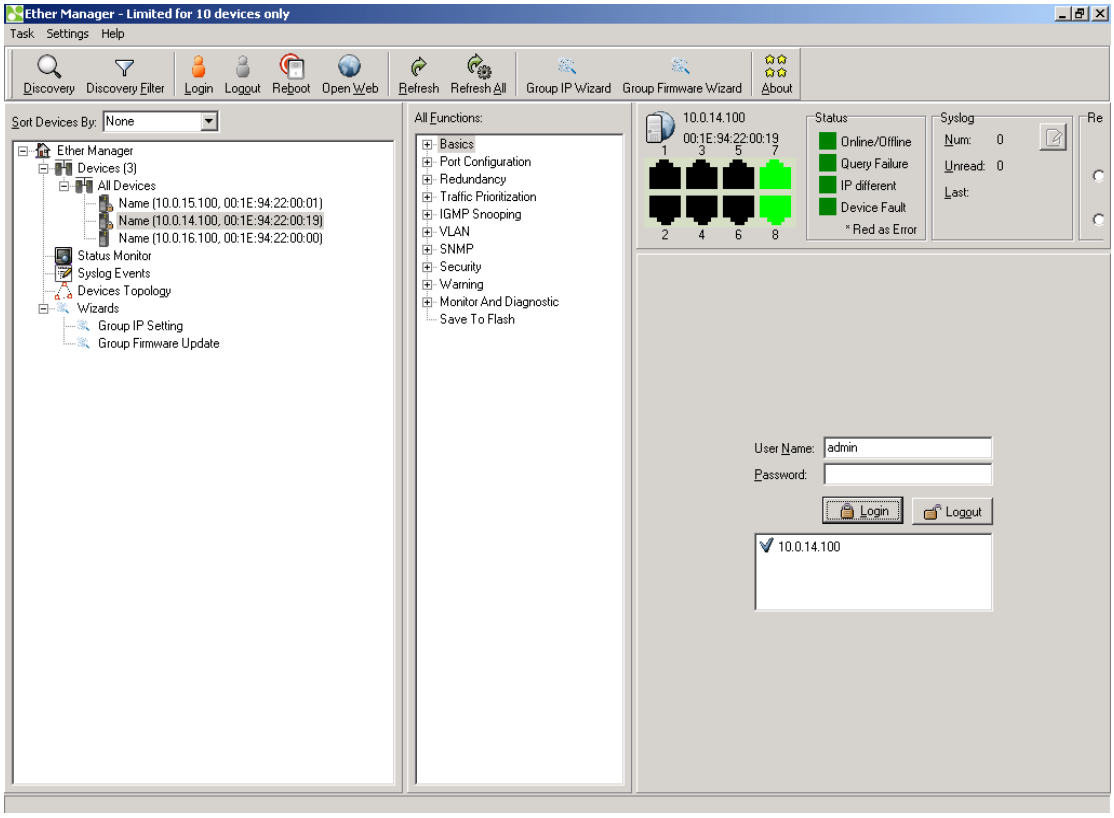
Appendix: Configuring with Atop's Utility Software: EtherManager

A.1 EtherManager Basics

A.1.1 EtherManager as Switch-management Tool

All EH switches are furnished with an Atop's utility program **EtherManager** that allows the user to configure, monitor and manage one or multiple switches at the same time.

After installing the program on the PC, an EtherManager window shall appear.

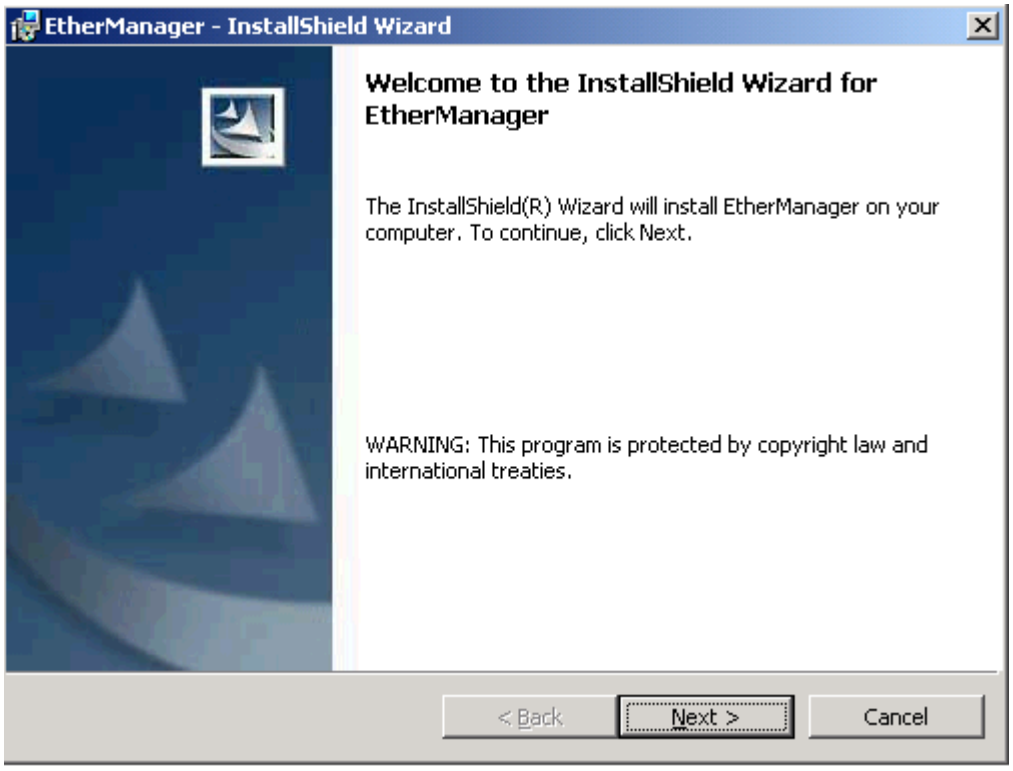


Example **EtherManager** Panel

A.1.2 Installing EtherManager

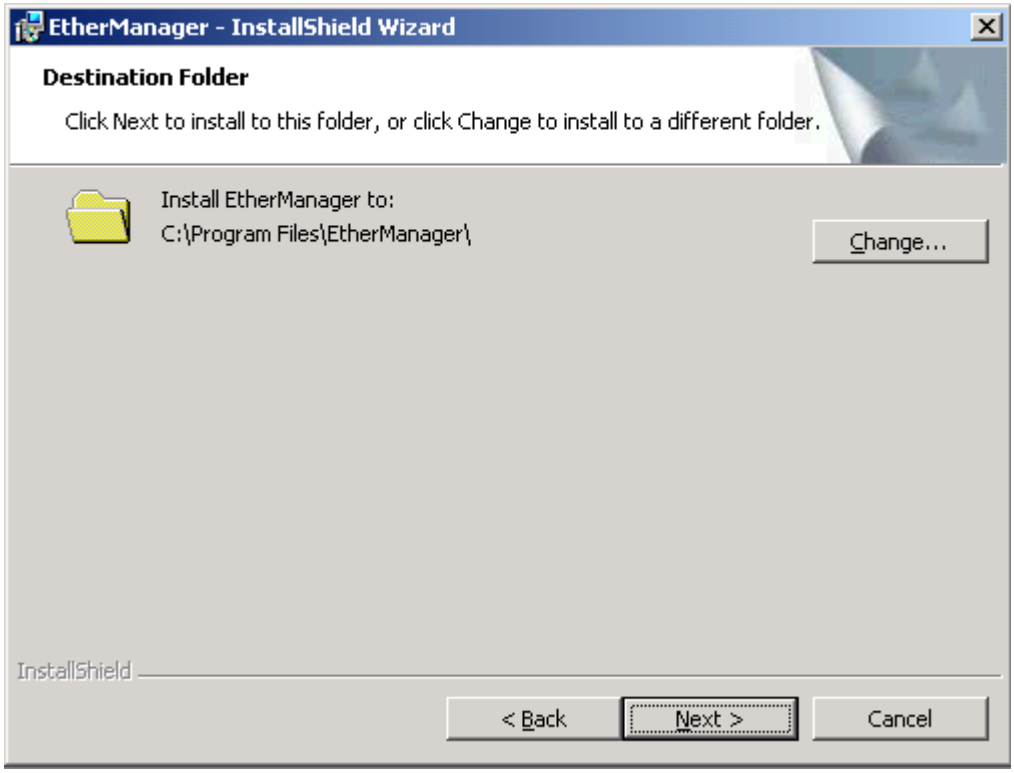
The **EtherManager** CD-ROM is furnished when an EH switch is delivered. First open the **EtherManager**.exe file on the CD, then follow the steps below.

Click **[Next]** when the following **Welcome** window appears.

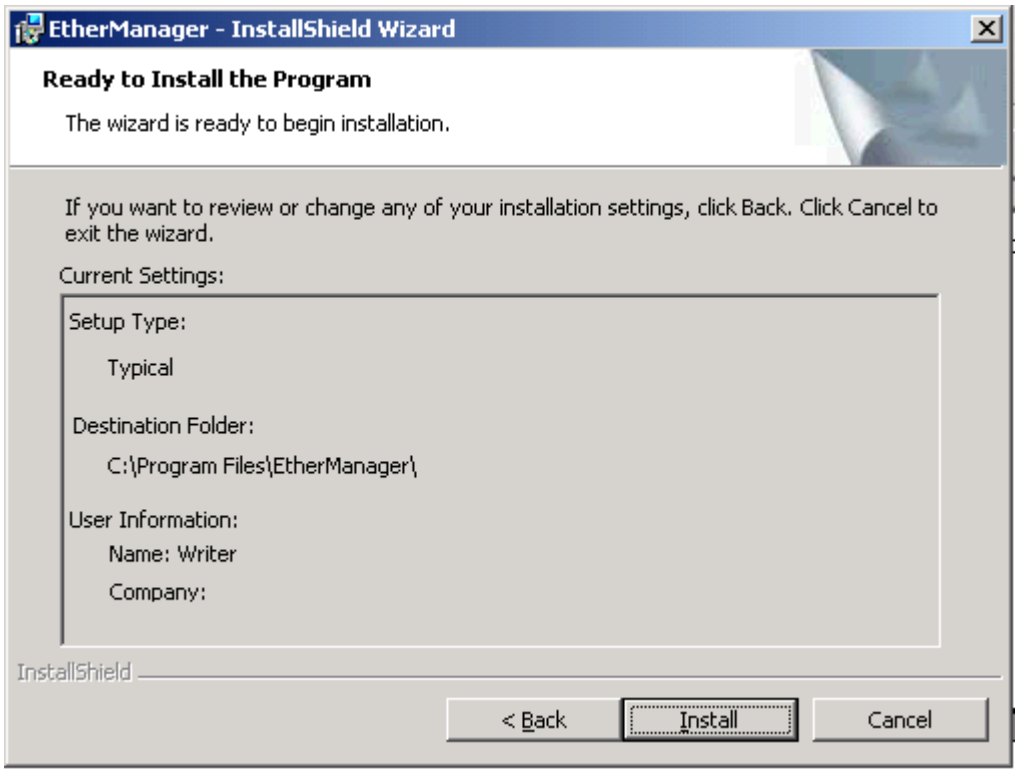

EtherManager - InstallShield Wizard
Welcome to the InstallShield Wizard for EtherManager
The InstallShield(R) Wizard will install EtherManager on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

When the window shown below appears, select the path that the user wants to install **EtherManager**. If the default path C:\Program Files**EtherManager** is acceptable, then click **[Next]** to continue**.**

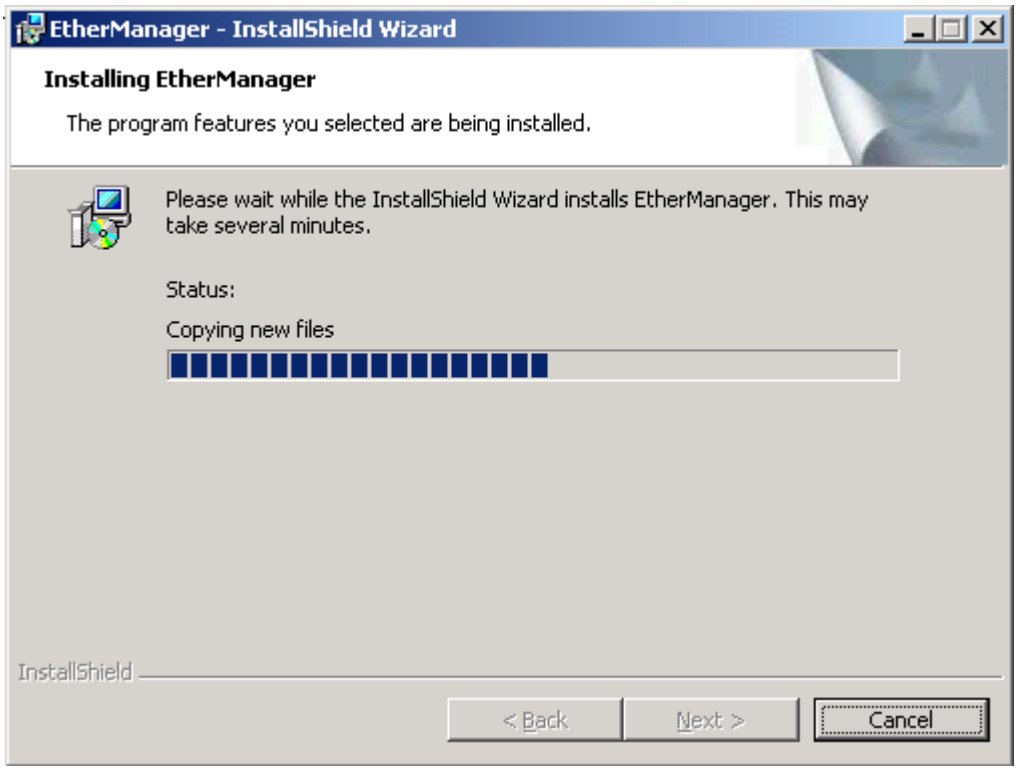
If the user wishes to change the path, then click [change] and go on.



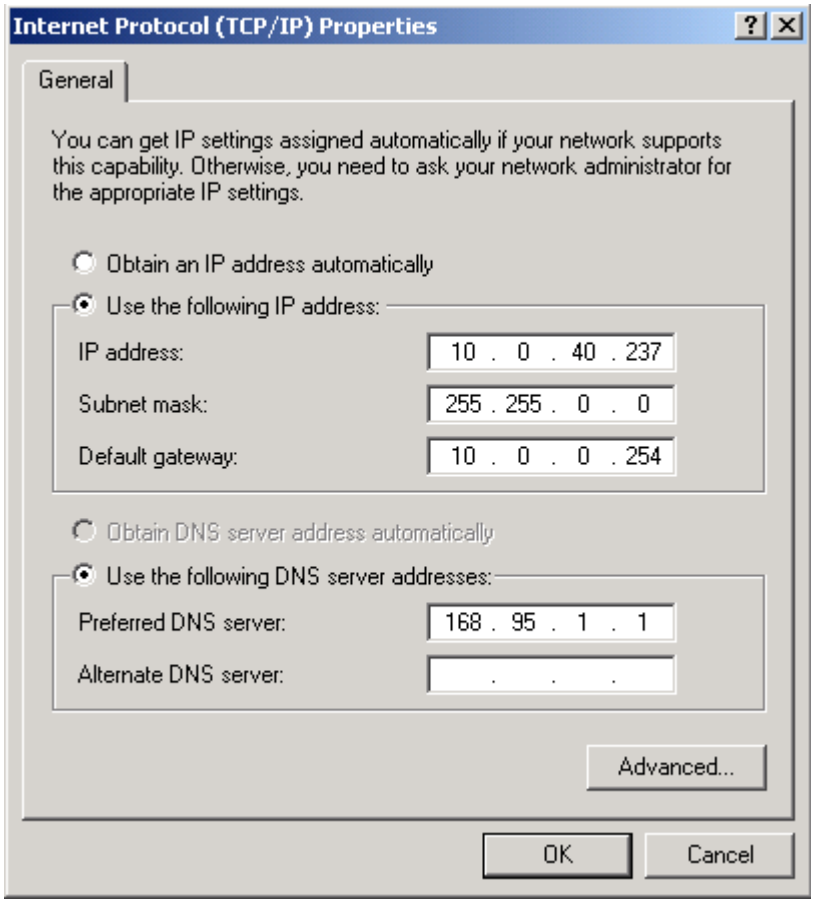
Once the path is selected, the following window shall appear.



Click **[install]** to confirm the installation.


EtherManager - InstallShield Wizard
Installing EtherManager
The program features you selected are being installed.
Please wait while the InstallShield Wizard installs EtherManager. This may take several minutes.
Status:
Copying new files
InstallShield
< Back
Next >
Cancel

Following the successful installation is a dialog box shown below. One may select to "**Obtain an IP address automatically**" if an EH switch has been installed on the same subnet as the user. If the user wishes to assign an IP address, then check "**Use the following IP address**:" box. The User's **IP address, Subnet mask** and **the Default gateway** addresses can be obtained by Windows' **Start->run->cmd->ipconfig** command. It is essential that the PC and the switch to be configured must be on the same subnet mask. The **DNS server address** can be your ISP DNS IP (for instance, 168.95.1.1 is Hinet's DNS server)


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 0 . 40 . 237
Subnet mask: 255 . 255 . 0 . 0
Default gateway: 10 . 0 . 0 . 254
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 168 . 95 . 1 . 1
Alternate DNS server:
Advanced...
OK
Cancel

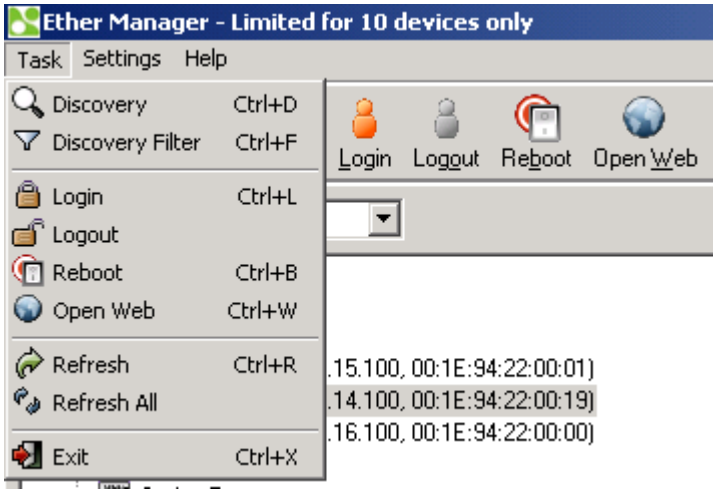
A.2 Tasks and Functions

A.2.1 DISCOVERY

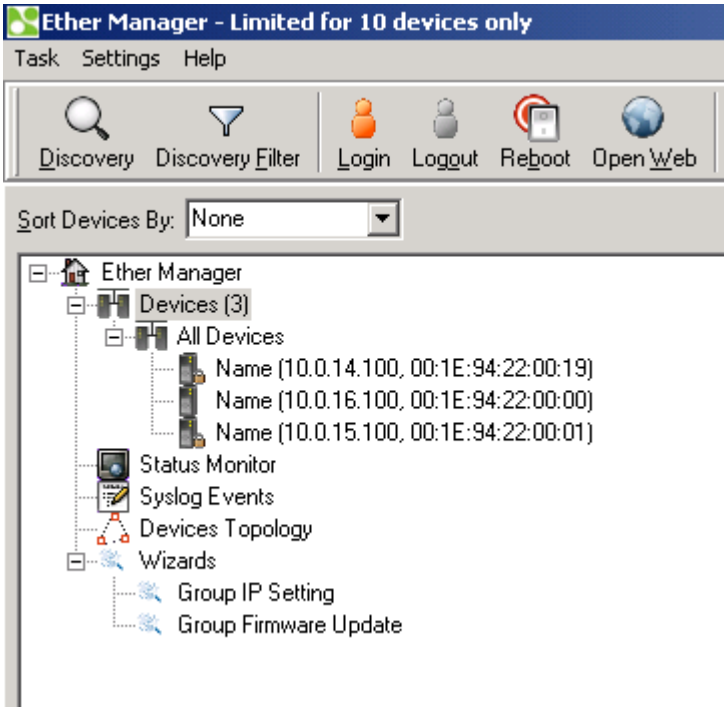
The user can select a task needed to be performed from the **task** pull-down menu or click the icon on the bar. The user can also click on the icon on the Task Bar for the following functions:

"Discovery, Discovery Filter, Login/out. reboot, Open Web, Refresh, and Refresh All".

First of all, one must click Discovery to "discover" what EH switches are on the subnet; or to narrow the search, one may apply a "Discovery Filter" to limit the search.

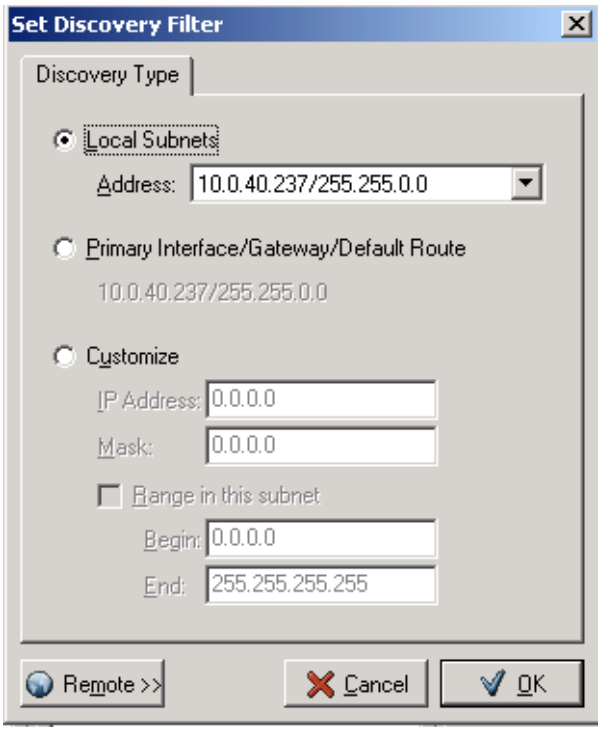


The searching can be done by selecting "**Discovery**" on the pull-down menu or simply click **Discovery** on the Task bar . A sample result is shown below, where three devices are found. They are "named" after their IP's and MAC Addresses.



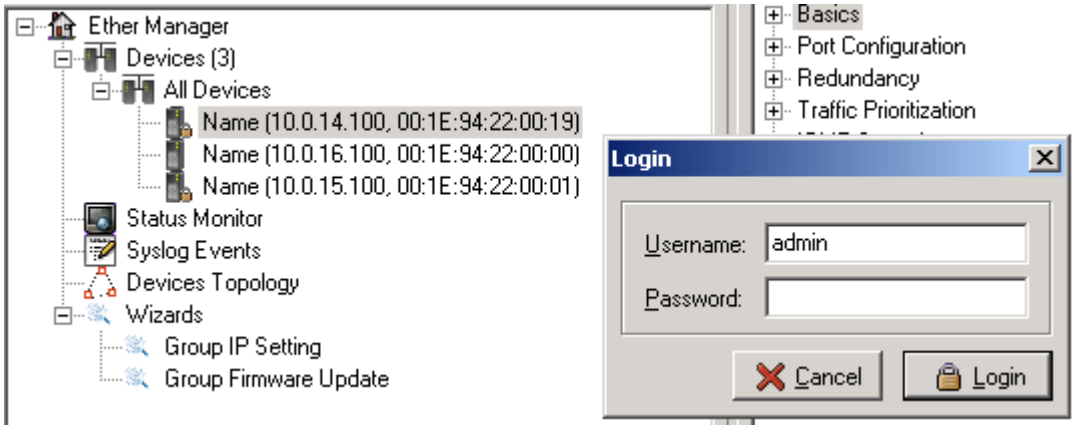
A.2.2 DISCOVERY FILTER

Click "**Discovery Filter**" and the following **"Discovery Type"** window shall pop up. Here one can set the filter to limit the searching (filtering) to just a given local subnet (shown as 10.0.40.237/255.255.0.0), or to search in a designated **"Primary Interface/Gateway/Default Route**", or to **customize** a **Discovery** range.



A.2.3. To Login and Logout

Once the "discovery" is done, the "discovered" switches will be displayed on the right-hand panel. Select by clicking the switch (device) to be worked on, then click **Login** to enter the login window before a managing session. When **login** is successful, the switch icon changes from to. If no task is assigned 30 seconds after login, the switch logouts itself automatically. One may click logout to do the same.



Login Interface

A.2.4 Reboot

The "**Reboot**" command forces a switch to reboot. A dialogue box will appear to reconfirm the command. After "Reboot", the user must go back to **Discovery** task to locate the devices again.

A.2.5 Open Web

The **Open Web** command opens the Web-based Interface if one prefers to perform the configuring online.

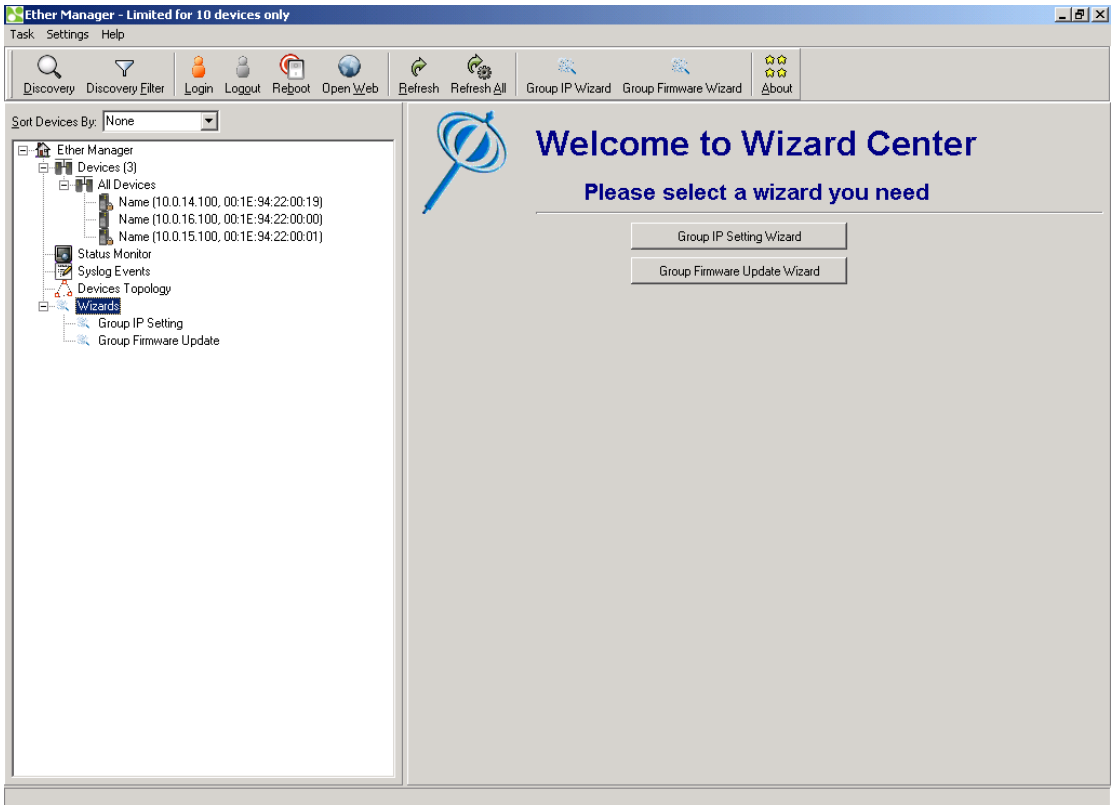
A.2.6 Refresh

Refresh forces a selected device to be updated immediately (displayed on the right panel).

Refresh All forces all discovered devices to be updated.

A.2.7 Wizards

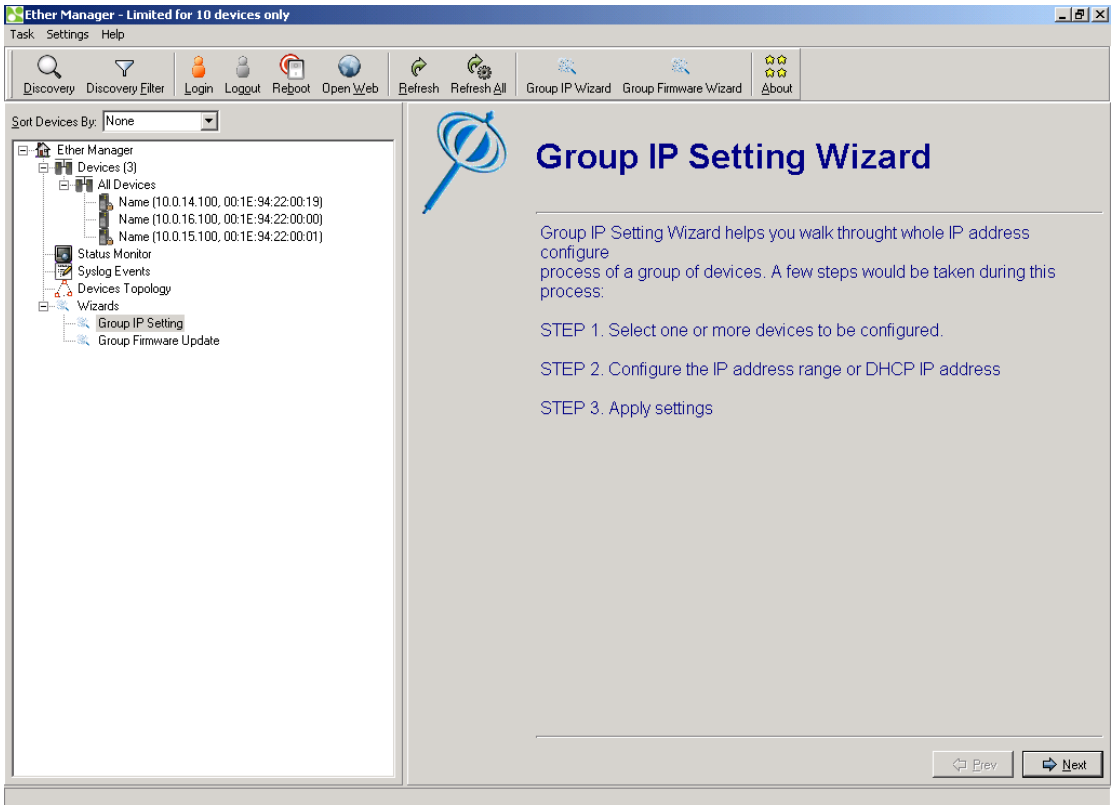
Two "Wizards" functions are provided to help the user to perform **Group IP setting** and **Group Firmware Update** tasks. The following window shall appear when "**Wizards**" button (left side of the panel) is clicked.


Ether Manager - Limited for 10 devices only
Task Settings Help
Discovery Discovery Filter Login Logout Reboot Open Web Refresh Refresh All Group IP Wizard Group Firmware Wizard About
Sort Devices By: None
Ether Manager
Devices (3)
All Devices
Name (10.0.14.100, 00:1E:94:22:00:19)
Name (10.0.16.100, 00:1E:94:22:00:00)
Name (10.0.15.100, 00:1E:94:22:00:01)
Status Monitor
Syslog Events
Devices Topology
Wizards
Group IP Setting
Group Firmware Update
Welcome to Wizard Center
Please select a wizard you need
Group IP Setting Wizard
Group Firmware Update Wizard

A.2.7.1 Group IP Setting Wizard

Wizards Interface

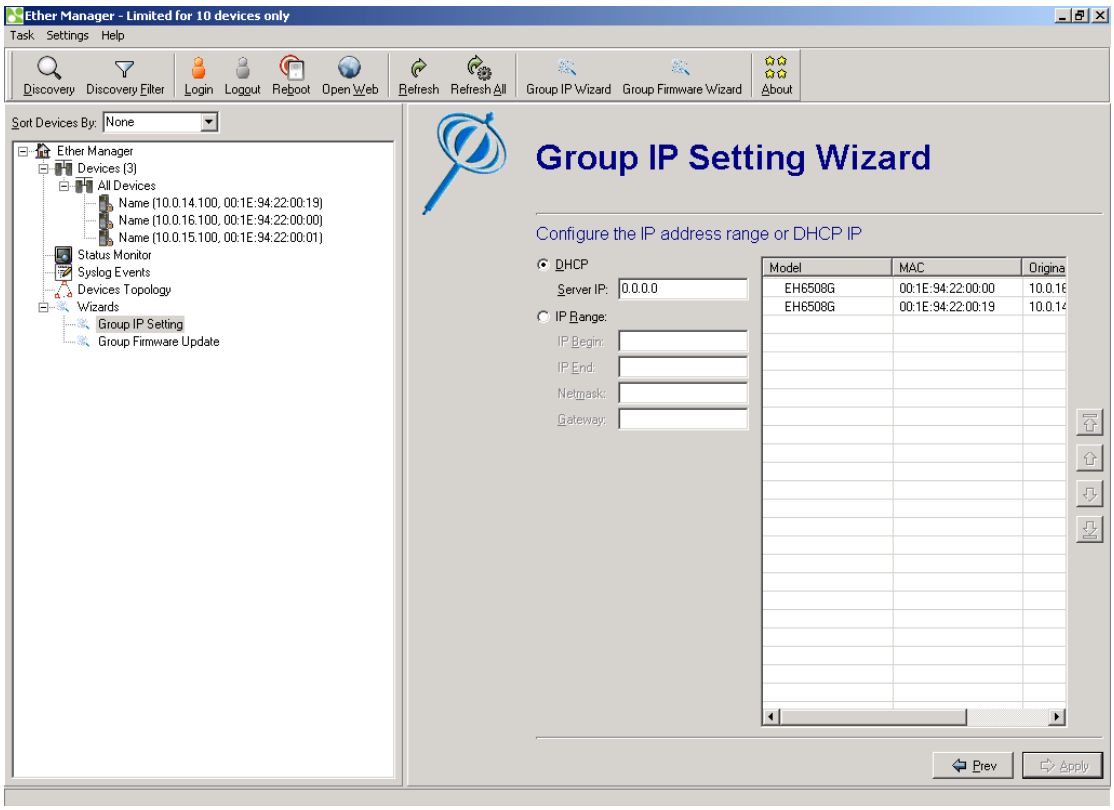
Group IP Setting Wizard assists the user through the entire **Group IP Setting** process.


Ether Manager - Limited for 10 devices only
Task Settings Help
Discovery Discovery Filter Login Logout Reboot Open Web Refresh Refresh All Group IP Wizard Group Firmware Wizard About
Sort Devices By: None
Ether Manager
Devices (3)
All Devices
Name (10.0.14.100, 00:1E:94:22:00:19)
Name (10.0.16.100, 00:1E:94:22:00:00)
Name (10.0.15.100, 00:1E:94:22:00:01)
Status Monitor
Syslog Events
Devices Topology
Wizards
Group IP Setting
Group Firmware Update
Group IP Setting Wizard
Group IP Setting Wizard helps you walk throught whole IP address configure
process of a group of devices. A few steps would be taken during this process:
STEP 1. Select one or more devices to be configured.
STEP 2. Configure the IP address range or DHCP IP address
STEP 3. Apply settings
Prev
Next

Group IP Setting Wizard Interface

STEP: 1. Select one or more devices to be configured, then press next to the sample panel appeared below.

STEP: 2. Configure the IP address range or DHCP IP address

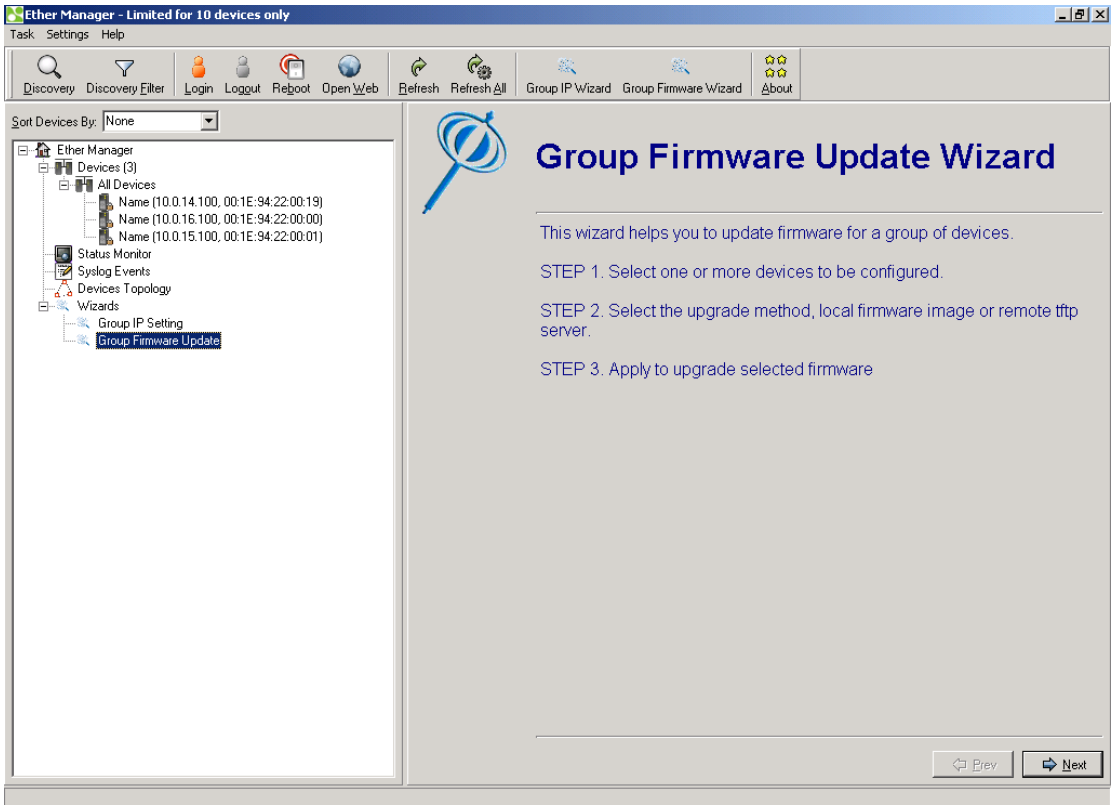


STEP: 3. **Apply** settings. Select **File->Save** to save the setup.

A.2.7.2 Group Firmware Update Wizard

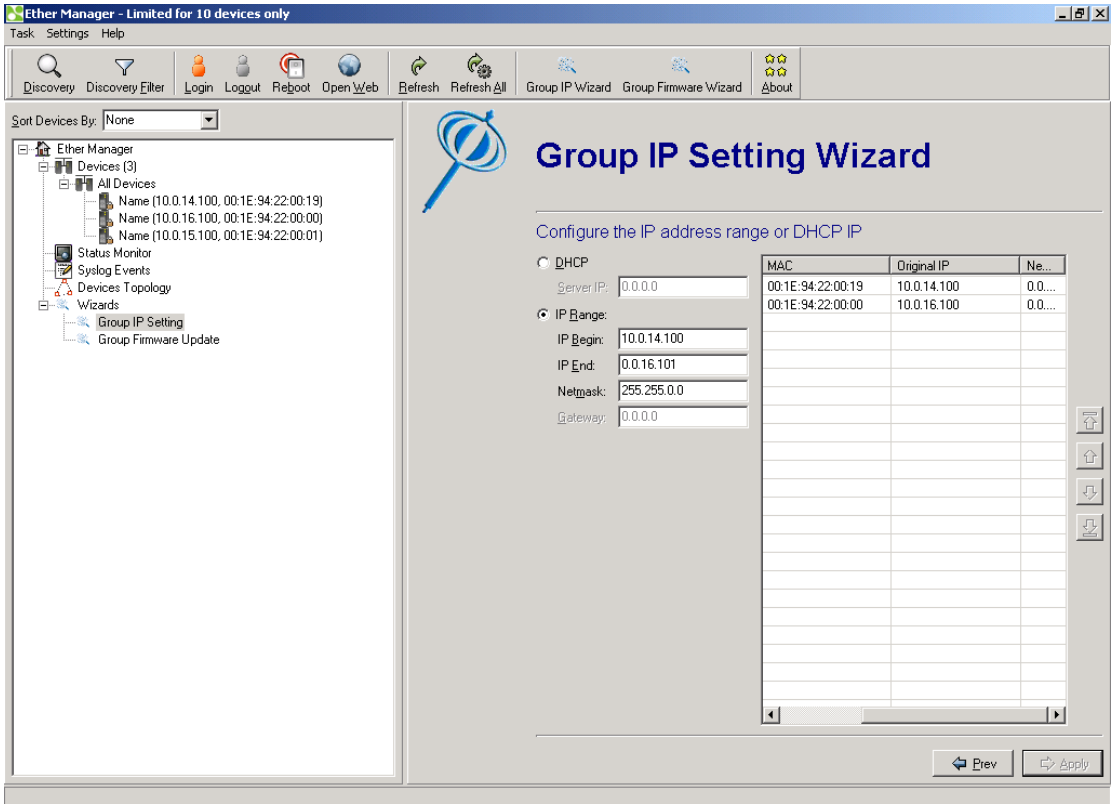
This wizard helps the user to update firmware for a group of devices simultaneously.

First click **Group Firmware Wizard** to pop up the following window.


Ether Manager - Limited for 10 devices only
Task Settings Help
Discovery Discovery Filter Login Logout Reboot Open Web Refresh Refresh All Group IP Wizard Group Firmware Wizard About
Sort Devices By: None
Ether Manager
Devices (3)
All Devices
Name (10.0.14.100, 00:1E:94:22:00:19)
Name (10.0.16.100, 00:1E:94:22:00:00)
Name (10.0.15.100, 00:1E:94:22:00:01)
Status Monitor
Syslog Events
Devices Topology
Wizards
Group IP Setting
Group Firmware Update
Group Firmware Update Wizard
This wizard helps you to update firmware for a group of devices.
STEP 1. Select one or more devices to be configured.
STEP 2. Select the upgrade method, local firmware image or remote tftp server.
STEP 3. Apply to upgrade selected firmware
Prev
Next

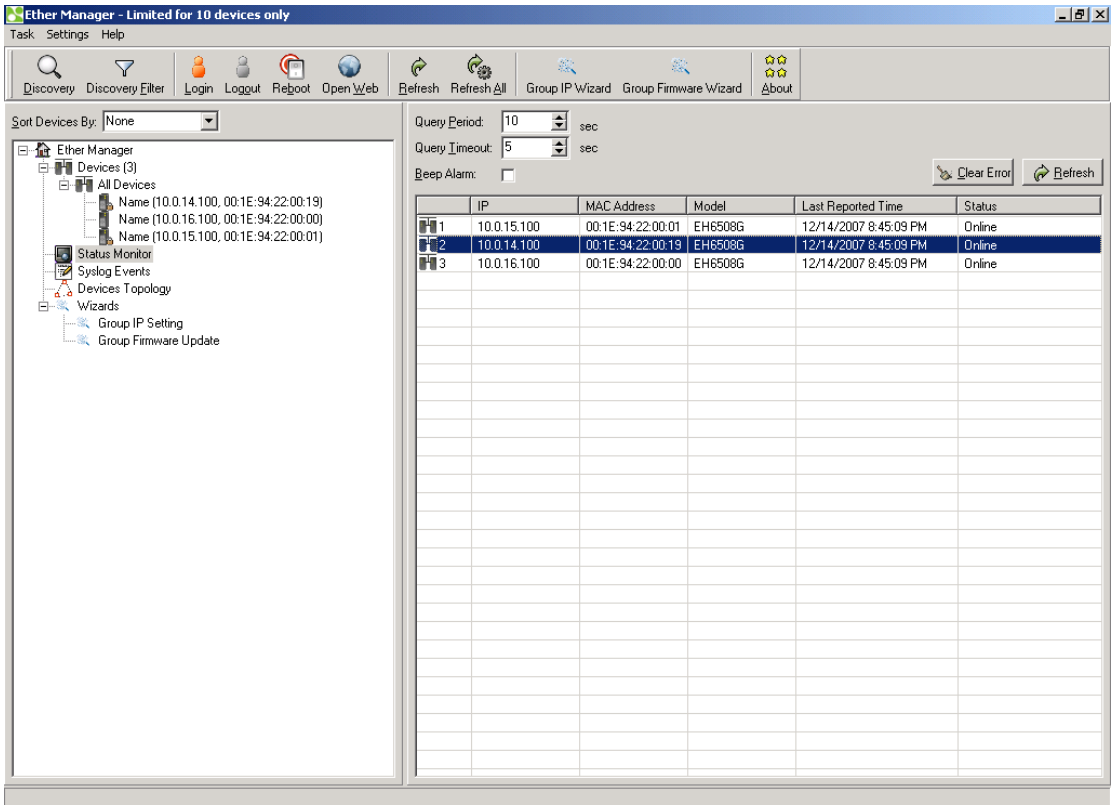
Group Firmware Update Wizard Interface

The procedure for **Group Firmware Update** is similar to that for **Group IP Setting**



A.2.8 STATUS MONITOR

Status Monitor allows the user to monitor all discovered switches in a tabulated form. Any color changes on a switch suggests a status change, and the user may want to review the events.

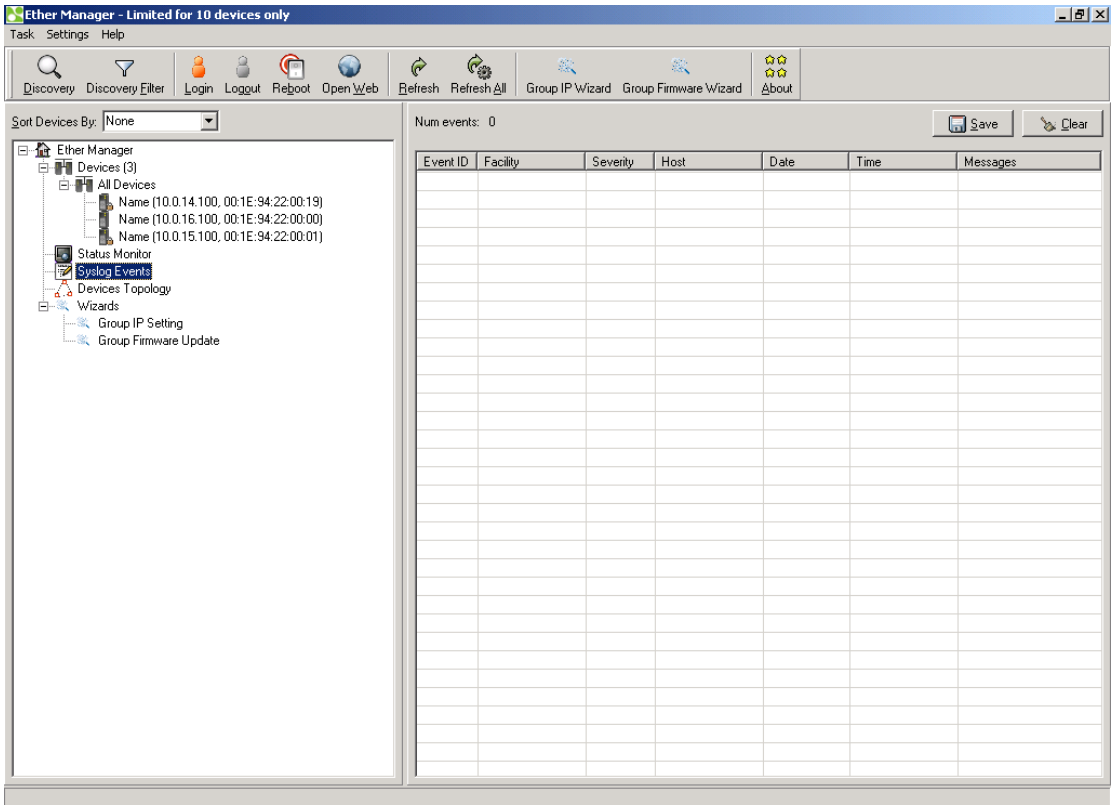

Ether Manager - Limited for 10 devices only
Task Settings Help
Discovery Discovery Filter Login Logout Reboot Open Web Refresh Refresh All Group IP Wizard Group Firmware Wizard About
Sort Devices By: None
Ether Manager
Devices (3)
All Devices
Name (10.0.14.100, 00:1E:94:22:00:19)
Name (10.0.16.100, 00:1E:94:22:00:00)
Name (10.0.15.100, 00:1E:94:22:00:01)
Status Monitor
Syslog Events
Devices Topology
Wizards
Group IP Setting
Group Firmware Update
Query Period: 10 sec
Query Timeout: 5 sec
Beep Alarm:
Clear Error
Refresh
IP MAC Address Model Last Reported Time Status
1 10.0.15.100 00:1E:94:22:00:01 EH6508G 12/14/2007 8:45:09 PM Online
2 10.0.14.100 00:1E:94:22:00:19 EH6508G 12/14/2007 8:45:09 PM Online
3 10.0.16.100 00:1E:94:22:00:00 EH6508G 12/14/2007 8:45:09 PM Online

Status Monitor Interface

Label	Description
Query Period	The period that **EtherManager** sends a packet to device to query status.
Query Timeout	Enter the timeout period, after which if **EtherManager** does not receive reply from device, a warning message will be displayed.
Beep Alarm	**EtherManager** will beep the PC to inform the user of new events.
Remove	Remove monitored device entry.
Refresh	Refresh the status.
IP	Display the IP Address of discovered switch.
MAC Address	Display the MAC Address of discovered switch.
Model	Display the Model name of discovered switch.
Last Reported Time	Display the last time that **EtherManager** receives report from switch.
Status	Display switch online/offline and show events alarm.

A.2.9 SYSLOG EVENTS

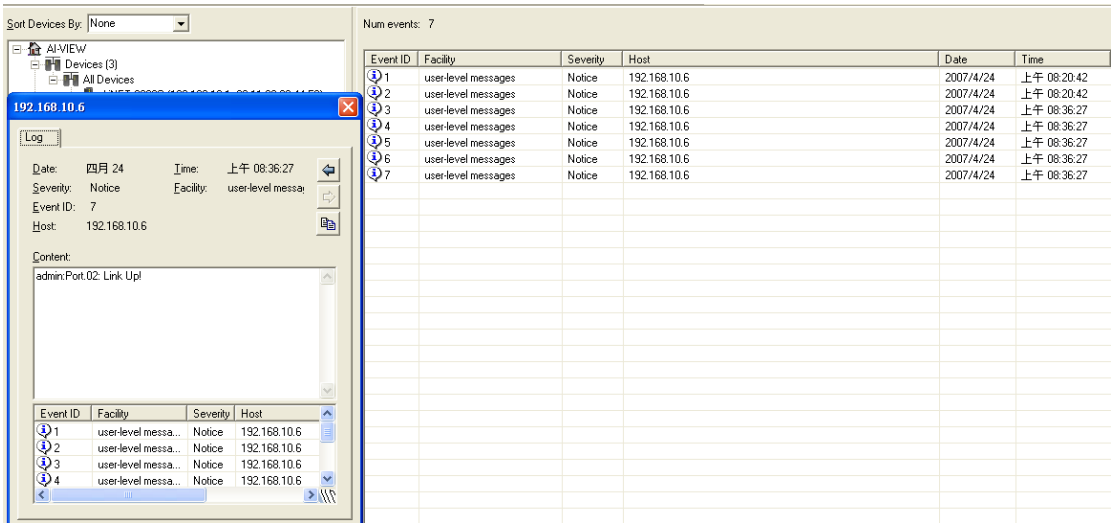
EtherManager has a built-in **Syslog Server**, and hence no other **Syslog** software is needed. **Syslog Events** displays all recorded events.



Syslog events Interface

Label	Description
Event ID	The number of events.
Facility	Class of the event.
Severity	The degree of severity.
Host	Event source address.
Date	Date of the event.
Time	Time of the event.

The user can view the detail event information by double clicking the event entry.


Sort Devices By: None
Num events: 7
Event ID Facility Severity Host Date Time
1 user-level messages Notice 192.168.10.6 2007/4/24 上午 08:20:42
2 user-level messages Notice 192.168.10.6 2007/4/24 上午 08:20:42
3 user-level messages Notice 192.168.10.6 2007/4/24 上午 08:36:27
4 user-level messages Notice 192.168.10.6 2007/4/24 上午 08:36:27
5 user-level messages Notice 192.168.10.6 2007/4/24 上午 08:36:27
6 user-level messages Notice 192.168.10.6 2007/4/24 上午 08:36:27
7 user-level messages Notice 192.168.10.6 2007/4/24 上午 08:36:27
192.168.10.6
Log
Date: 四月 24
Time: 上午 08:36:27
Severity: Notice
Facility: user-level messa
Event ID: 7
Host: 192.168.10.6
Content:
admin:Port.02: Link Up!

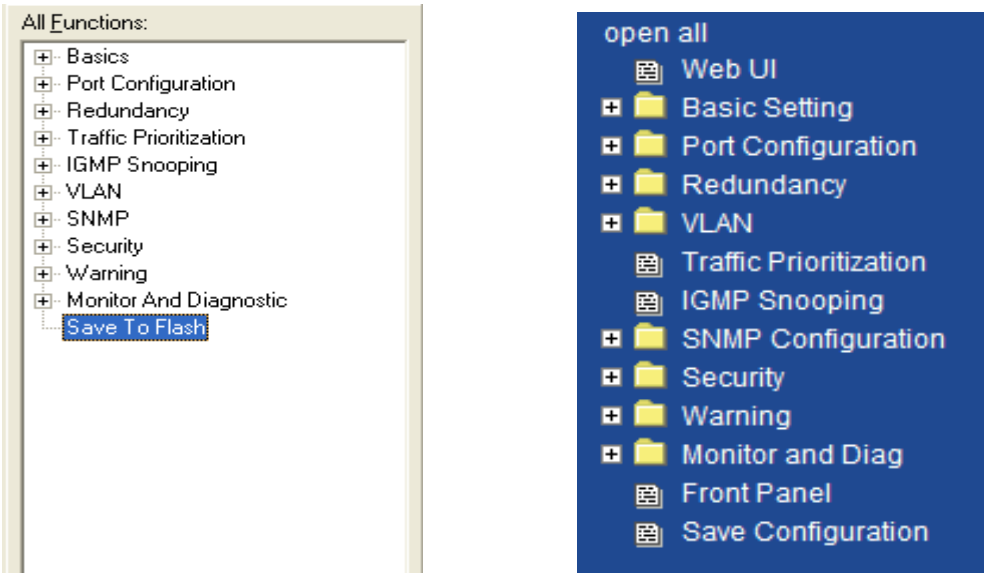
Detail events Interface

Icon	Description
	Previous event.
	Next event.
	Copy event content to clipboard.
	Leave the window.

A.3 All-Functions Interfaces

A.3.1 "ALL-FUNCTIONS" MENU AND WEB-BASED MANAGEMENT FUNCTIONS

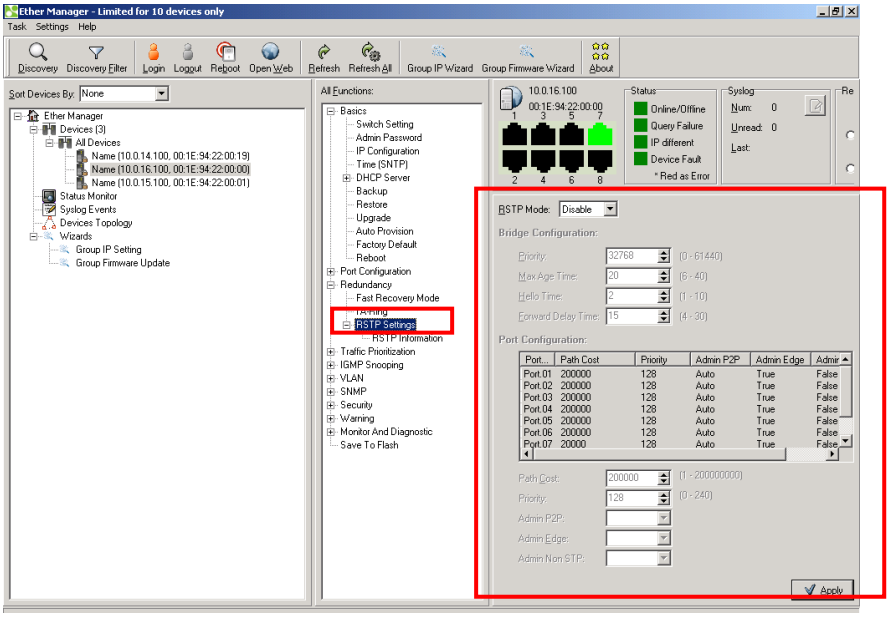
The "**All Functions**" menu is similar to that in the **Web-based** management: any feature that can be found on the **Web-based** management can be done using **EtherManager**'s "**All-Functions**" Menu. The diagram juxtaposes the "**All Functions**" panel (on the left) and the equivalent **Web-based** management panel (on the right) to show their similarity.



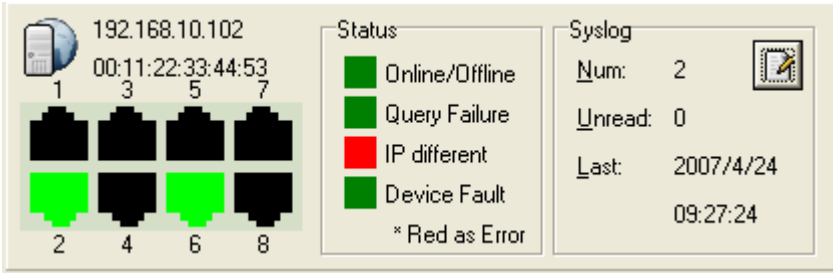
The functions interface and functions tree on WEB.

A.3.2 CONFIGURING WITH THE "ALL FUNCTIONS" MENU (AN EXAMPLE)

When the user selects a specific function to configure, the selected setting(s) shall appear on the right part of the display panel. In the example below, **RSTP** is selected for configuration:



On the display panel shown above, the user can view the switch status in an enlarged picture shown below.



EH6508G Technical Specifications

Technology	
Ethernet Standard	802.3-10BaseT, 802.3u-100BaseTX, 100BaseFX, 802.3x- 802.3z-1000BaseLX, 802.3ab-1000BaseTX, 802.3ad-, 802.1d-MAC Bridges, 802.1d-, 802.1p-Class of Service, 802.1q-, 802.1w-Rapid Spanning Tree Protocol, 802.1x-Port Based Network Access Control
MAC address	8192
Priority Queue	4
Flow Control	IEEE 802.3x Flow Control and Back-pressure
Processing	Store-and-Forward
Interfaces	
RJ-45 Port	6 x 10/100 Base-T(X), Auto MDI/MDI-X
Giga Fiber Port (Model EH 6508G-Fm or EH6508G-Fs; m for multi-mode, s for single mode)	2 x 1000 Base-X (SC Connector) Multi-Mode: 850 nm, max 550m Single mode:1310 nm, max 2 km
Giga Port (copper) (Model EH6508G)	2 x 10/100/1000 Base-T(X), Auto MDI/MDIX
LED Indicator	**PWR1, PWR2, and PWR3** (Green) **Fault** RJ45 Ports (6): **LNK/ACT** (Green/Blinking Green), Full duplex(Amber) Giga Ports (2; copper): **LNK/ACT** (Green),Link (Amber)
Power	
Power Input Voltage	**PWR1/ PWR2**: 12~48VDC in a 6-pin Terminal Block **PWR3**: 12~45VDC in Power Jack
Reverse Polarity Protection	Yes
Power Consumption	9 Watts Max
Environmental	
Operating Temperature	-10 to 60℃
Storage Temperature	-40 to 85℃
Operating Humidity	5% to 95%；Non-condensing
Mechanical	
Dimensions (W x D x H)	52 mm (W) x 106 mm (D)x 144 mm (H)
Casing	IP-30 protection
Regulatory Conformance	
Regulatory Standards	CE class A RoHS
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), Level 3, EN61000-4-6 (CS), Level 3
Shock	IEC60068-2-27
Free Fall	IEC 60068-2-32
Vibration	IEC 60068-2-6